Micro-ordinateurs,
informations, idées, trucs et astuces

Utiliser l'Internet

Auteur : ***François CHAUSSON***
Date : ***27 novembre 2008***
Référence : ***Internet_utiliser.doc***

Préambule

Voici quelques informations utiles réunies ici initialement pour un usage personnel en espérant qu'elles puissent aider d'autres utilisateurs de micro-informatique.

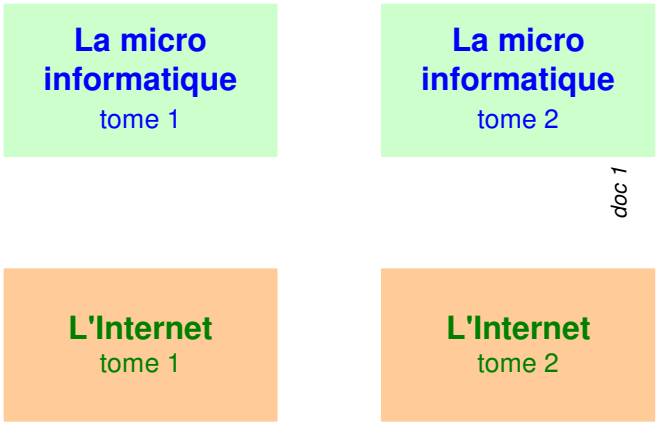
Ces informations sont présentées sans démarche pédagogique ; si un niveau de détail était nécessaire sur un sujet particulier, ne pas hésiter à me demander.

Ce document

Ce document traite de **sujets Internet**.

Il fait partie de l'ensemble documentaire ***Micro-ordinateurs, informations, idées, trucs et astuces*** qui couvre ces sujets :

1. *La micro-informatique*, en 2 tomes
2. *L'Internet*, en 2 tomes



3. *Des Trucs HTML et Javascript*
4. *Des notices d'utilisation de divers logiciels*[1]

Tout commentaire à propos de ce document pourrait être adressé à :
pcinfosmicro@francois.chausson.name

Ce document est régulièrement mis à jour sur : http://fcfamille.free.fr/[2]

[1] ZoneAlarm, AVG, …
[2] Site à accès contrôlé

Table des matières

Ce qui n'est pas dans ce document

- Les *Virus* : voir le document *PC_infos_micro 1.doc* puisque Internet n'est pas le seul vecteur des virus
- Tout ce qui est dans le tome 2, afin d'éviter de rendre ce tome 1 trop volumineux

Internet, Web, mail, etc…

Comme ces termes ne sont pas équivalents, même si l'un est parfois utilisé pour l'autre, il peut être utile de commencer par un petit tour :

- *Internet* : c'est le moyen de transport de tout, le tuyau technique par lequel passent toutes les informations
- *Web* : pour accéder à des sites Web et en *consulter* des pages
- *Messagerie* : pour *échanger* des messages
- *Transfert de fichiers* : pour *envoyer* des fichiers à un destinataire, par exemple à l'hébergeur de son site Web
- …

Une démarche simple

En prenant ces sujets au pas à pas et en passant par une analogie ferroviaire[3] :

La situation de départ de l'utilisateur

« Je dispose d'un micro-ordinateur »	Analogie : « J'habite une maison »

Le besoin de l'utilisateur

« Je souhaite pouvoir me connecter à Internet »	Analogie : « Je souhaite pouvoir utiliser la SNCF »

Le lien initial

« J'établis une **connexion** avec un PAI (Prestataire d'Accès Internet) »	Analogie : « Je contacte la SNCF »

Erreur! Aucune rubrique spécifiée.

Une visite

« Je vais voir la Tour Eiffel sur le **site Web** de la Ville de Paris »	Analogie : « Je prend le train pour aller à Paris voir la Tour Eiffel »

Erreur! Aucune rubrique spécifiée.

Un courrier

« J'envoie un **mail** à un interlocuteur, je lis sa réponse »	Analogie : « Ma lettre, donnée à La Poste, prend le train pour être livrée à mon correspondant, sa réponse prend le même chemin »

Erreur! Aucune rubrique spécifiée.

[3] dans les deux cas, l'utilisateur passe par un réseau

Quelques informations complémentaires

Des langages

Sans le savoir, l'utilisateur « parle » au réseau, à Internet donc, un langage à chaque fois spécifique de l'utilisation qu'il en fait :

- Messagerie : protocole SMTP
- Web : protocole HTTP[4]
- Transfert de fichiers : protocole FTP[56]

Il existe encore d'autres « languages », comme SOAP pour les Web Services, ...

L'inventeur

A chaque inventeur son invention :

- *L'Internet* : par les militaires américains soucieux de disposer d'un réseau de communication fiable en cas d'attaque adverse[7]
- Le *Web* : par le CERN[8] à Genève pour permettre à des non-résidents d'accéder à des données techniques élaborées dans les sous-sols des contreforts des Alpes et de l'environnement immédiat de ll'aéroport de Genève

En conclusion

[4] ce qui s'affiche dans les en-têtes d'URL dans la fenêtre du navigateur, en haut à gauche
[55] voir « Publier le site » plus loin
[6] à noter qu'un Navigateur sait "parler" FTP
[7] soviétique à ce moment là
[8] immense centre de recherche de physique fondamentale

Accéder à Internet

Il faut disposer de :
- *un prestataire d'accès Internet*[9], p.9
- *une connexion physique*[10], p.9
- *un logiciel Navigateur*, p. 13

Le prestataire d'accès Internet

Globalement, les prestataires peuvent être initialement[11] partagés en deux groupes :
- *les prestataires payants*
  comme Wanadoo, Easynet, AOL, …
- *les prestataires gratuits*[12]
  comme Free, Libertysurf, …

Outre le coût, d'autres caractéristiques sont à considérer :
- la rapidité de la connexion
- la taille maximum de la messagerie
- la surface disque fournie au niveau du serveur du PAI pour un éventuel site Web
- la qualité du support[13]
- l'impact éventuel de la publicité sur le confort de la connexion (messages non sollicités, …)

Les coûts sont de plusieurs ordres :
- *l'abonnement*
  par exemple, l'abonnement Easynet annuel par connexion téléphonique en 2002 se montait à 72 Euros.
- *les communications téléphoniques pour contacter le serveur du PAI*
  si la connexion se fait de cette manière
- *l'achat du modem*[14]
  en particulier pour l'ADSL ou le câble

Remarques :
- AOL fournit/impose l'utilisation d'une interface propriétaire[15] qui a pour effet d'« enfermer » l'utilisateur dans un environnement et un outil spécifiques

La connexion physique

La connexion physique peut être :
- *la ligne téléphonique habituelle*[16]
- *le câble*

[9] dit PAI
[10] une ligne téléphonique, le câble, …
[11] à l'expérience, d'autres critères peuvent devenir dominants
[12] bien voir ce qui est gratuit parmi les différents coûts et ce qui peut rester payant
[13] souvent médiocre
[14] qui est souvent constitué d'une carte ajoutée dans le micro
[15] plutôt que de laisser chacun utiliser les outils habituels : Internet explorer, Outlook express, Eudora, …
[16] en concurrence avec les appels téléphoniques normaux

- *l'ADSL*
- *Des formules spécialisées :*
  - *Courant porteur en ligne (CPL),* par EDF ou d'autres
  - *Satellite,* avec parabole et modem spécialisé
  - *Wimax, du* haut-débit par voie hertzienne[17]

La rapidité de la connexion

La rapidité de la connexion n'a pratiquement pas d'impact sur les utilisations de la messagerie puisque les volumes échangés sont en général faibles, de l'ordre de quelques centaines de Koctets[18], sauf si un message était accompagné d'une pièce attachée un peu volumineuse.

Par contre, les accès Web nécessitent toujours des transferts beaucoup plus volumineux[19] et plaident en faveur de transferts rapides ; ceci est d'autant plus vrai si l'utilisateur souhaite s'en servir souvent et longtemps.

Sur une ligne téléphonique, des modems à 28.000 bps[20], plutôt 56.000 bps maintenant, sont le plus souvent utilisés ; ils conviennent normalement pour des utilisateurs débutants ou occasionnels.

Le câble ou l'ADSL permettent des transferts beaucoup plus rapides et sont destinés à des utilisateurs très actifs : 128 Mbps, 512 Mbps, ….

Attention quand même que toutes les solutions de connexion ne sont pas fonctionnellement équivalentes.

Le câble, par exemple, n'est disponible[21] que en ville ; cette solution, qui peut être bonne dans ce seul contexte, ne fonctionnerait pas dans une résidence secondaire par exemple.

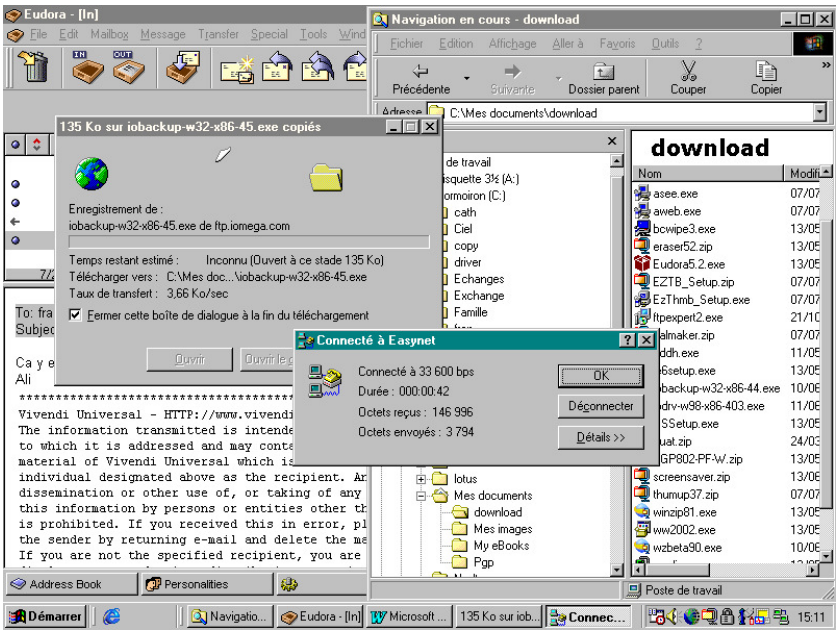
Egalement, l'ADSL n'est pas actuellement disponible en dehors des villes tant que les centraux en province n'auront pas été amenés au bon niveau technologique.

Temps de transfert

Pour du texte, les transferts concernent naturellement des caractères ; ceux ci sont codés en ASCII[22], utilisant ainsi 7 bits par caractère.

Dans la pratique, pour tenir compte d'échanges complémentaires, on utilise non pas un ratio de 7 mais de 10 environ ; ceci veut dire qu'une liaison, par exemple à 31.200 bps[23], transférera environ 3,6 kOctets à la seconde.

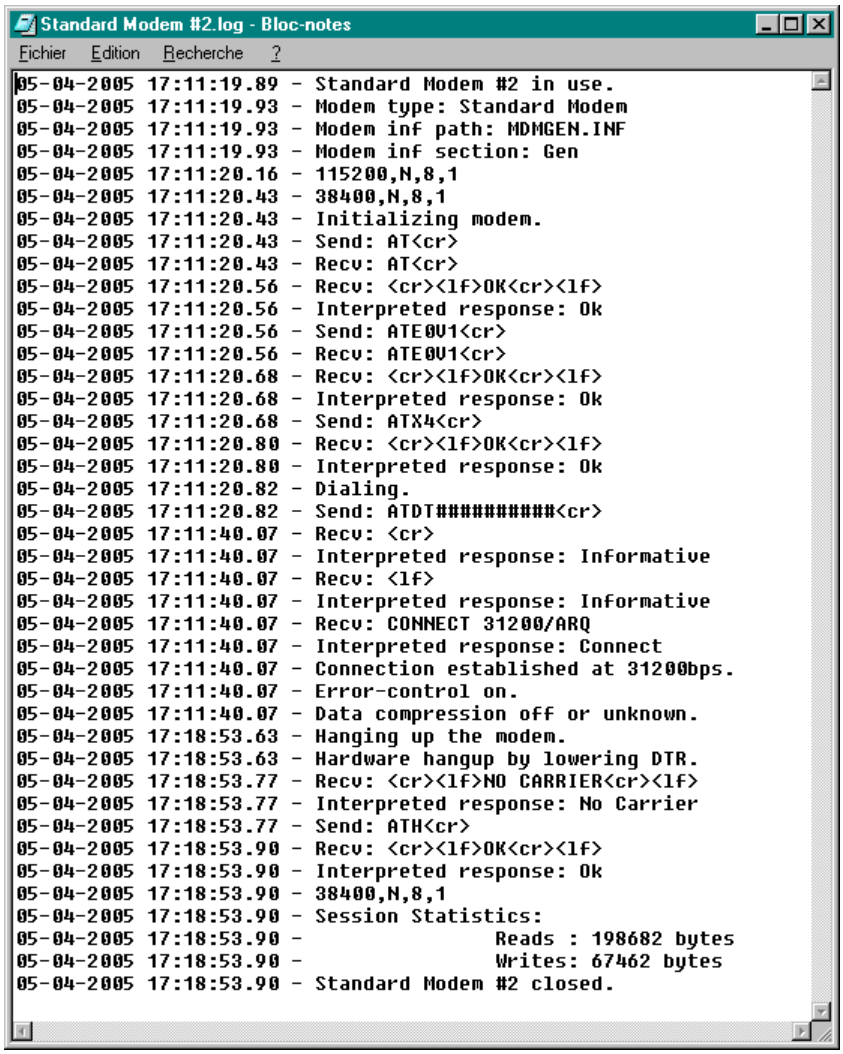
[17] plusieurs dizaines de Mbits sur plusieurs dizaines de kms
[18] Ko : voir « Glossaire technique »
[19] au minimum, plusieurs Meg
[20] bits par seconde
[21] en gros
[22] ASCII : voir « Glossaire technique »
[23] par exemple, à Mormoiron



Ainsi, un message comportant une pièce attachée de 2Meg mettra environ 10 minutes à être émis ou reçu.

Une connexion téléphonique

Voici le dialogue technique normal enregistré dans le fichier *Log* du modem :



Remarques :

- cet exemple peut servir pour réaliser une comparaison avec le contenu du fichier Log relatif à un échange qui se serait terminé en erreur

Une connexion ADSL

Un avantage de l'ADSL sur le câble est de pouvoir faire transférer géographiquement, si besoin était, sa connexion ADSL pourvu toutefois que la région de destination soit équipée ADSL[24].

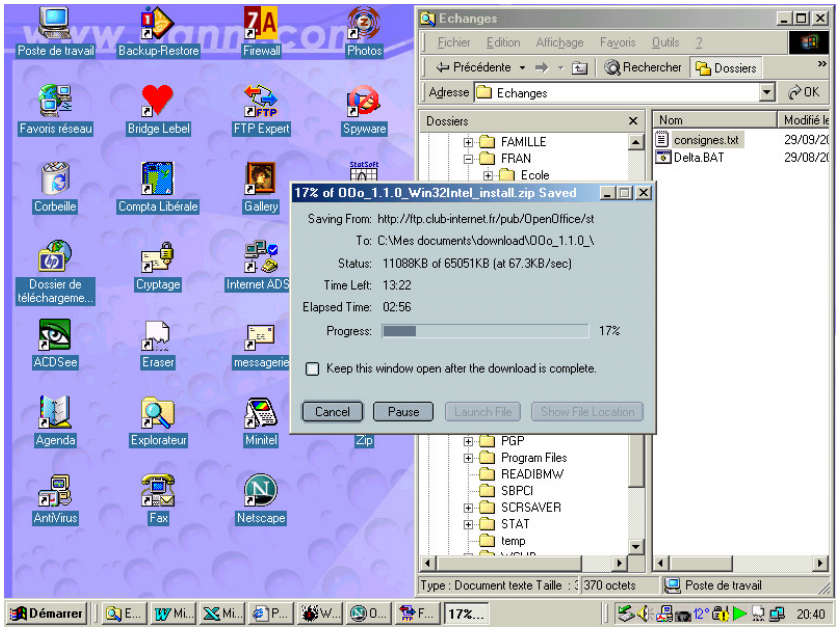
Une raison pour prendre son contrat ADSL chez son PAI habituel est de ne pas avoir à changer d'adresse(s)[25], ou bien au minimum de ne pas avoir à faire rediriger sa messagerie de son PAI vers son accès ADSL ; une autre raison est que le tarif groupé, messagerie et accès ADSL chez le même, est parfois moins élevé que la somme de deux tarifs séparés chez deux PAI différents.

Egalement, bien que l'ADSL utilise la ligne téléphonique, les conversations téléphoniques se font simultanément à la connexion Internet ; la modulation des fréquences y pourvoit.

[24] vérifier sur www.netissimo.tm.fr sur la base du code postal de la commune
[25] voir aussi « Une adresse pérenne »

Equipé d'une connexion ADSL rapide, il devient rapidement évident que le goulot d'étranglement est alors souvent transféré de l'autre coté, sur les sites accédés, ou une partie inconnue du réseau, qui ne peuvent pas toujours dialoguer à ces vitesses élevées.

Voici un exemple de téléchargement avec l'ADSL :



réalisé à 67.000 car., soit environ 20 fois plus rapidement que l'exemple précédent.

Paramétrages

En venant d'une connexion téléphonique normale vers l'ADSL ou le câble, penser à modifier les paramétrages dans :

- le logiciel de messagerie : Outlook, Eudora, etc..
- le browser : IE, Netscape, …

Voir aussi des exemples de paramétrages en annexe.

En même temps ?

Il est possible[26] d'utiliser simultanément une connexion RTC et une connexion ADSL au même prestataire[27].

Simplement, le user utilisé ne doit pas être le même.

Le « bouchon » ADSL

Il faut mettre un filtre à chaque prise téléphonique utilisée[28].

Le filtre s'attaque aux hautes fréquences :

- connexion téléphonique : seules les basses fréquences passent
- connexion ADSL : tout passe

[26] au moins chez Easyconnect

[27] situation rencontrée en testant la mise en œuvre d'une connexion RTC tout en ayant oublié de fermer la connexion ADSL chez le même prestataire

[28] à l'inverse, c'est inutile sur une prise non utilisée

S'il manque un filtre :

- connexion téléphonique : des sifflements gênants mais pas bloquants
- connexion ADSL : des ruptures de synchronisation de la Freebox, qui provoquent son reboot

En mettre partout ?

Pas forcément, par exemple :

- une alarme qui appelle en cas de déclenchement[29] : si la Freebox est éteinte[30], il n'y aura pas d'impact
- une commande de chauffage à distance : vérifier que les hautes fréquences ne la déclenchent pas ; si Oui, mettre un filtre

Dégrouper or not ?

Un utilisateur ADSL peut être :

- en dégroupage partiel
- en dégroupage total

Dans le premier cas, il a conservé sa ligne et son / ses poste(s) téléphonique(s) France Telecom[31].

Dans le deuxième cas, il les a supprimés pour n'avoir plus qu'un téléphone connecté à sa « Box »[32][33].

La question

Faut-il aller au dégroupage total ?

Les raisons pour y aller

- faire l'économie de l'abonnement FT, soit 16-17[E/]mois, en utilisant un / plusieurs téléphone(s) connecté(s) à sa Box
- pour un utilisateur équipé d'un portable, la panne de téléphone de Box n'est pas bloquante

Les raisons pour ne pas y aller

- la Box peut tomber en panne interne, tomber sur une panne d'alimentation électrique[34], …
- si la Box est en panne, le dépannage nécessite d'appeler la Hot Line du PAI, un appel qui coûterait cher avec un portable[35]

Des sujets à éclaircir

- avec une alarme connectée, celle-ci fonctionnerait-elle sur un téléphone de Box ? dans les deux sens[36]
- avec une commande de chauffage à distance connectée, celle-ci fonctionnerait-elle sur un téléphone de Box ?

---

[29] si l'alarme est administrable à distance, avec des échanges en sens inverse donc, vérifier
[30] ce qui paraît vraisemblable en cas d'absence prolongée
[31] Qu'il utilisera pour les appels entrants
[32] Freebox, Livebox, …
[33] cette discussion exclut toute utilisation d'une Box sans sortie téléphone (modem pur)
[34] à l'inverse, un téléphone filaire fonctionne toujours
[35] et serait impossible depuis une cabine téléphonique
[36] appel de l'alarme ? gestion de la centrale à distance ?

Le Navigateur

L'accès aux sites Web se fait avec un navigateur :

- *Internet Explorer*
- *Netscape*, pour le temps où il existe encore
- d'autres encore: *Opera*, *Safari* ou encore *Firefox*

aux mérites très comparables même si IE est parfois plus fiable sans être extraordinaire.

En savoir plus

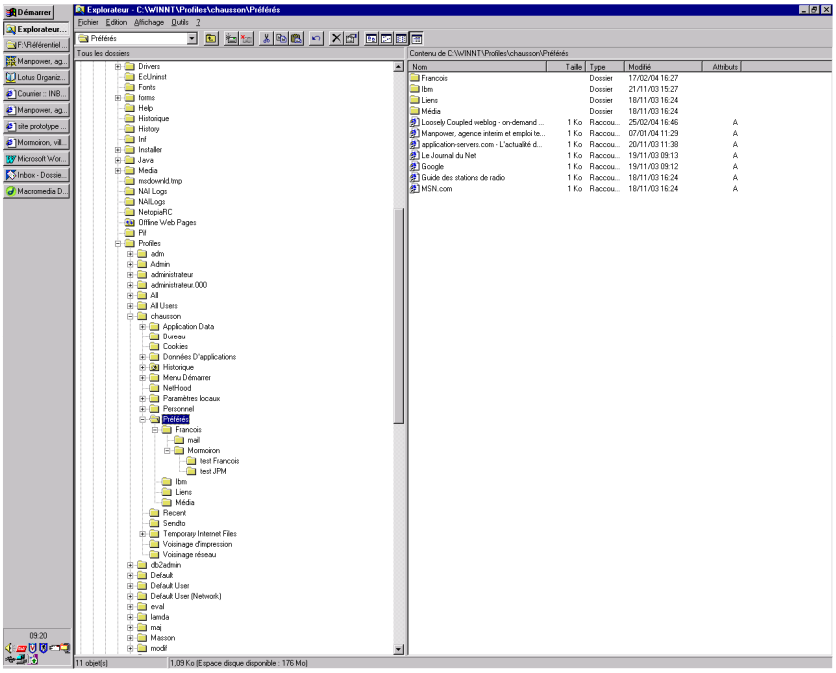
Voir le document *Utiliser Internet Explorer.doc*.

Les Favoris

Pour conserver les URL des sites Web intéressants.

Ces Favoris sont:

- capturés dans le Navigateur par *Favoris/Ajouter aux favoris*
- stokés dans *C:/Windows/Profiles/*nom_de_connexion*/Preferes/*



montré ici avec un WinNT.

L'adresse IP

Chaque utilisateur d'Internet connecté a une adresse qui lui est propre, l'*adresse IP*.

Cette adresse est de la forme, par exemple :

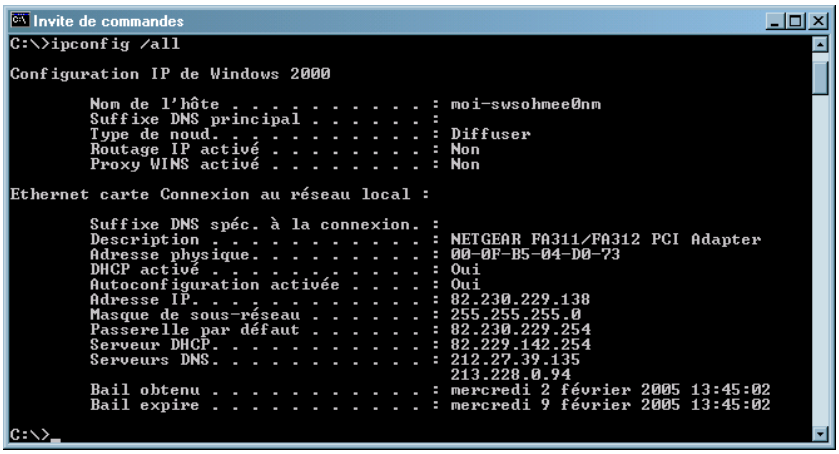
82.230.229.138

comportant toujours 4 nombres séparés par un point à chaque fois.

Connaître son adresse

Dans une fenêtre DOS, faire :

ipconfig /all



Adresse fixe et adresse dynamique

Adresse Internet[37]

Le PC de l'internaute

Tous les utilisateurs courants d'Internet ont une adresse IP qui leur est attribuée automatiquement[38] lors de leur connexion, une adresse IP *dynamique*[39].

En effet, il n'y a pas assez d'adresses disponibles pour en attribuer une à chacun qu'il soit connecté ou pas[40] ; seuls ceux qui sont connectés ont une adresse affectée.

Autant dire que le même PC n'aura pas, le plus souvent, la même adresse IP lors de deux connexions distinctes.

A noter que c'est un élément favorable en terme de sécurité de n'avoir pas toujours la même adresse.

Les serveurs

A l'inverse, tous les serveurs[41] ont une adresse IP *fixe* pour pouvoir y accéder.

En effet, pour initialiser une connexion, l'internaute désigne le serveur qu'il souhaite accéder par une URL[42], comme www.free.fr.

Les serveurs techniques de l'Internet[43] convertissent alors cet URL en une adresse IP[44], ce qui permet à la connexion d'aboutir ; à noter que[45] les serveurs DNS ne peuvent pas être désignés par un nom symbolique mais uniquement par une adresse IP.

Il existe plusieurs moyens pour obtenir une adresse IP fixe :

- demander à son PAI, quitte à la payer s'il la facture

[37] = externe
[38] par un mécanisme qui s'appelle le DHCP
[39] sauf ceux qui ont demandé une adresse fixe
[40] l'adressage actuel, en IP v4, permet 4,2 milliards d'adresses mais ça ne suffit pas
[41] Google, Wanadoo, SNCF, …
[42] URL : Universal Resource Locator
[43] les serveurs DNS
[44] qui doit donc être fixe
[45] = syndrome de la poule et de l'œuf, en quelque sorte

- utiliser une *Freebox* récente en dégroupé
- utiliser les services d'un prestataire[46] comme *NoIP* qui fait relais

Adresse Interne[47]

Pourquoi ?

Pour différentes raisons, comme de participer à du *Port Forwarding*.

Comment ?

Voir par ailleurs en annexe.

[46] = Dynamic DNS (DynDNS)
[47] dans un réseau local

Choisir une messagerie

L'échange de messages est une des utilisations principales d'Internet, une autre étant l'accès aux sites Web.

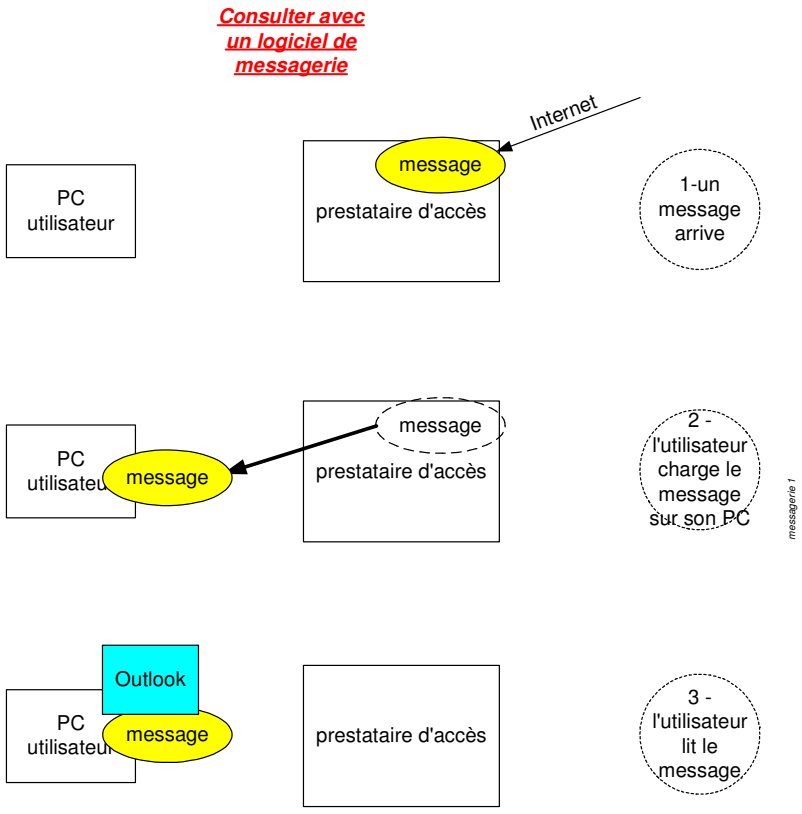
L'accès

Deux possibilités d'accès sont offertes :

- *par un logiciel spécialisé de messagerie*, p. 18
  le moyen le plus classique
  par exemple : Eudora, Outlook[48], …
- *par un site Web offrant ce service,* p. 19
  depuis son prestataire
  par exemple : Wanadoo, Easynet, Free, La Poste, …

Un logiciel de messagerie

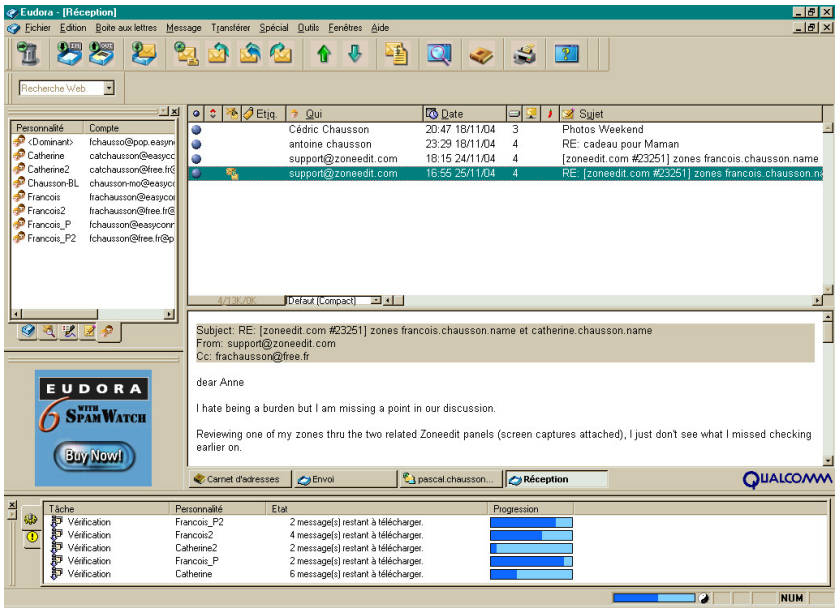
L'utilisateur installe sur son PC un logiciel de messagerie pour lire/écrire ses messages ; la démarche générale d'utilisation est illustrée ici :



Le logiciel Eudora, par exemple, peut être utilisé en mode « Sponsored », c'est à dire de manière gratuite au prix d'un petit panneau publicitaire pas bien gênant.

Ce logiciel peut être téléchargé depuis de nombreux sites, comme **www.tucows.com**.

[48] de Microsoft



Il est installé sur le micro de l'utilisateur.

En savoir plus

Voir les documents *Utiliser Outloot express.doc, Utiliser Eudora.doc*.

Des paramétrages

L'utilisation d'un logiciel de messagerie commence par quelques paramétrages.

Il faut savoir que :

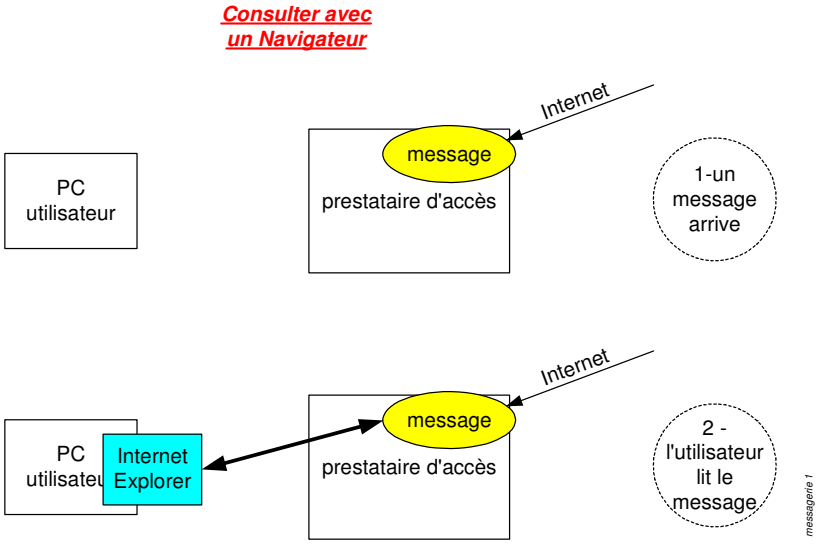
- le serveur POP3 : la fonction « serveur »[49] qui stocke les messages « entrants » jusqu'à la prochaine connexion par le logiciel de messagerie
  ex. de paramétrage de son adresse à Wanadoo : *pop3.wanadoo.fr*
- le serveur SMTP : la fonction serveur qui permet d'envoyer des messages « sortants »
  ex. de paramétrage de son adresse à Wanadoo : *smtp.wanadoo.fr*

Accéder à sa messagerie depuis le Web

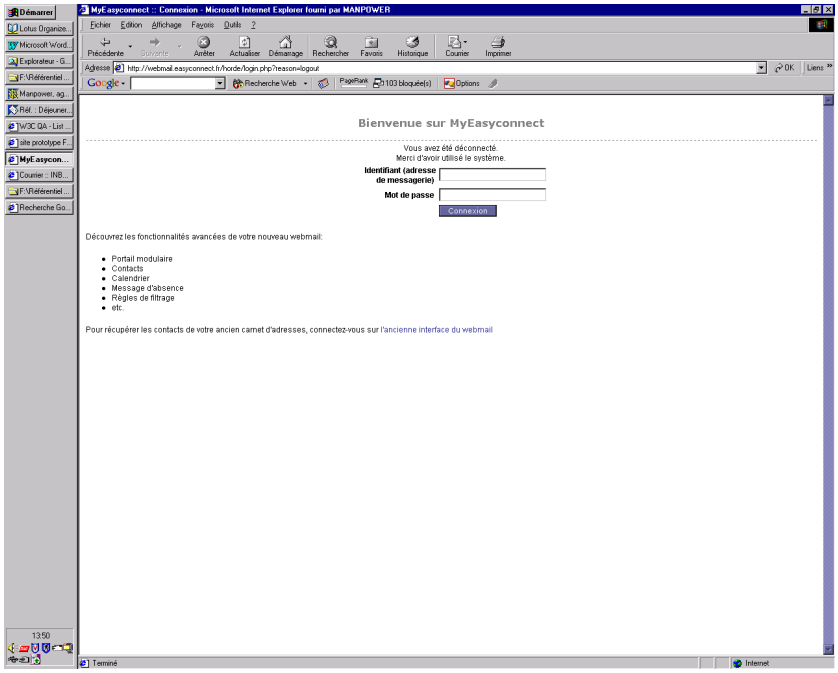
L'utilisateur passe par son Navigateur habituel pour lire/écrire ses messages, c'est le *WebMail*.

La démarche générale d'utilisation est illustrée ici :

[49] chez le PAI



En prenant comme exemple la messagerie de Easynet, il suffit de se connecter sur le site Web de Easynet[50] :



à l'adresse http://webmail.easyconnect.fr pour pouvoir consulter exactement le même courrier que celui qui pouvait être vu au travers de Eudora dans l'exemple précédent.

Une utilisation possible

Ca permet d'aller consulter sa messagerie personnelle depuis son bureau en allant sur le site Web[51] de son PAI.

Quelques inconvénients toutefois en limitent l'utilisation :

- pas d'accès au *AddressBook* existant sur le micro de l'utilisateur

[50] valable aussi avec les principaux PAI comme Wanadoo, etc …
[51] pour autant que l'entreprise autorise les accès Web, comme ça se pratique de plus en plus

- pas d'enregistrement dans les *Mailbox* sur le même micro de l'utilisateur

Un avantage :
- une bonne « isolation » des virus apportés par la messagerie[52]

Plusieurs adresses de messagerie

A l'usage, il s'avère rapidement utile d'avoir plusieurs adresses de messagerie.

Comme une adresse de messagerie est attribuée suivant le principe « premier arrivé/premier servi », il peut être intelligent de demander des adresses chez plusieurs PAI sans en avoir le besoin immédiat.

Chez le même PAI

Une idée est souvent d'avoir des adresses différentes pour :
- chaque membre de la famille
- une adresse professionnelle à coté d'une adresse personnelle
- …

Chez plusieurs PAI différents

Il peut aussi être utile d'avoir une adresse chez deux ou trois PAI différents, à La Poste, chez Free, etc, …

Un PAI « collecteur »

Il est possible d'indiquer à un PAI qu'il collecte tous les messages arrivant normalement chez d'autres PAI ; de cette manière, tous les messages arrivent chez un seul PAI et il n'est donc pas nécessaire de relever ses courriers chez chacun en en faisant le tour.

Un exemple

Habitant en ville, il peut être pratique d'utiliser le câble et d'avoir donc une adresse chez Noos.

Allant en vacances, il peut être également utile d'avoir un accès par ligne commutée téléphonique chez un PAI classique.

Dans ce cas, il serait pratique de choisir son prestataire câble comme collecteur de messagerie.

Un autre exemple

Après avoir été chez un PAI et avoir diffusé son adresse de messagerie à de nombreux correspondants, il peut être utile de la conserver pendant quelques mois après être allé chez un autre PAI.

Dans ce cas aussi, il sera utile de choisir son deuxième prestataire comme collecteur de messagerie.

Faire de la redirection d'adresse soi-même

Il est aussi possible de mettre en place sa propre gestion des adresses en redirigeant différentes messageries chez un même prestataire ; voir « Une adresse de messagerie pérenne », p.36.

[52] le seul élément technique actif sur le micro est la page HTML de visualisation

Et les virus ?

Pour commencer, rappelons que l'introduction d'un virus sur un poste de travail nécessite l'exécution d'un peu de code ; en gros, ça ne se fait pas tout seul.

Ainsi, de manière générale, un virus arrive par la messagerie par une pièce attachée[53] ; il faut pour cela ouvrir la pièce attachée et permettre l'exécution de code, par exemple du code d'une macro Word.

Il est théoriquement possible d'attraper un virus en consultant une page Web encore que ce cas soit rare ; même si le code HTML ne s'y prête pas, le code d'une page peut être dynamique[54] et permettre ainsi à un virus de s'introduire sur le poste de travail.

Pour finir, les recommandations sont :

- supprimer directement tout message dont l'émetteur est inconnu, même si le titre est accrocheur[55]
- ne jamais ouvrir une pièce attachée d'une provenance qui ne soit pas sûre[56]

Voir le document *PC_infos_micro 1.doc.*

Et la confidentialité ?

La confidentialité des mails n'est pas du tout certaine ; disons même qu'il ne faut absolument pas compter dessus si le besoin s'en faisait sentir.

En effet, il est beaucoup plus facile, techniquement et financièrement, de « lire » un mail que d'écouter une conversation téléphonique ou d'intercepter un courrier postal.

Les autorités compétentes[57] disposent sans aucun doute de logiciels spécialisés capables de recherches par mots clés[58] par exemple, voire en suivant d'autres logiques qui rendent l'interception d'un mail et la compréhension de son contenu un jeu d'enfant.

Leur problème est bien plutôt la trop grande quantité d'information plutôt que l'inverse.

Un moyen quand même

Le cryptage d'un mail permet d'en assurer la confidentialité[59].

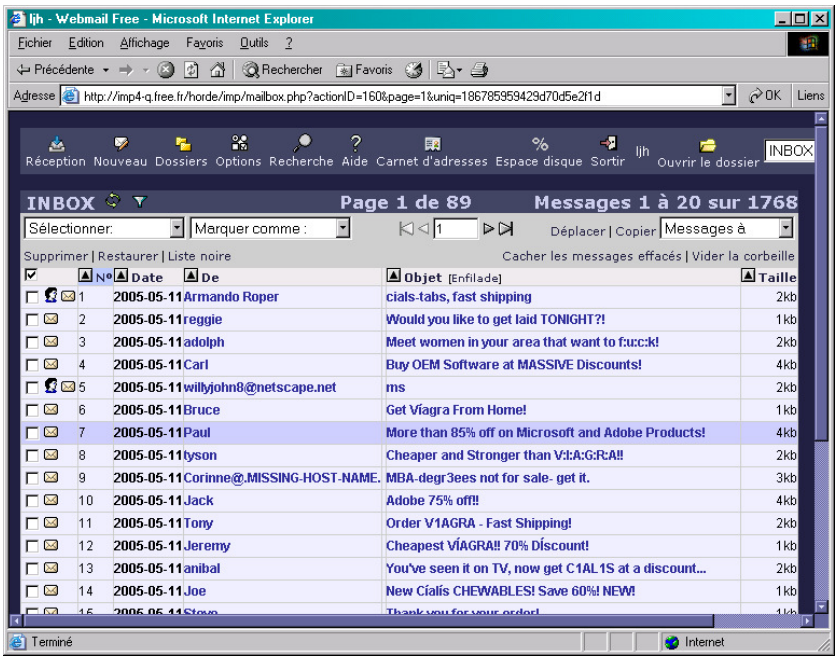
Combattre le Spam

Une des plaies de la messagerie est le Spam, qui consiste à recevoir des tombereaux de messages non sollicités qu'il faut ensuite éliminer pour pouvoir retrouver les quelques messages utiles.

Un exemple :

---

[53] visualiser un message n'est normalement pas suffisant à un virus pour se diffuser
[54] voir ASP, PHP, …
[55] de tous genres : « correctif Microsoft », « la Croix rouge française », …
[56] pour un document « texte », demander une version .RTF
[57] d'autres aussi d'ailleurs
[58] « cocaïne », « pédophilie », …
[59] voir le document *PC_infos_micro 2.doc*



Ce user mail chez Free a été de toute évidence pris pour cible par des spammer et environ 1800 messages se sont retrouvés là en quelques jours.

Des démarches anti spam

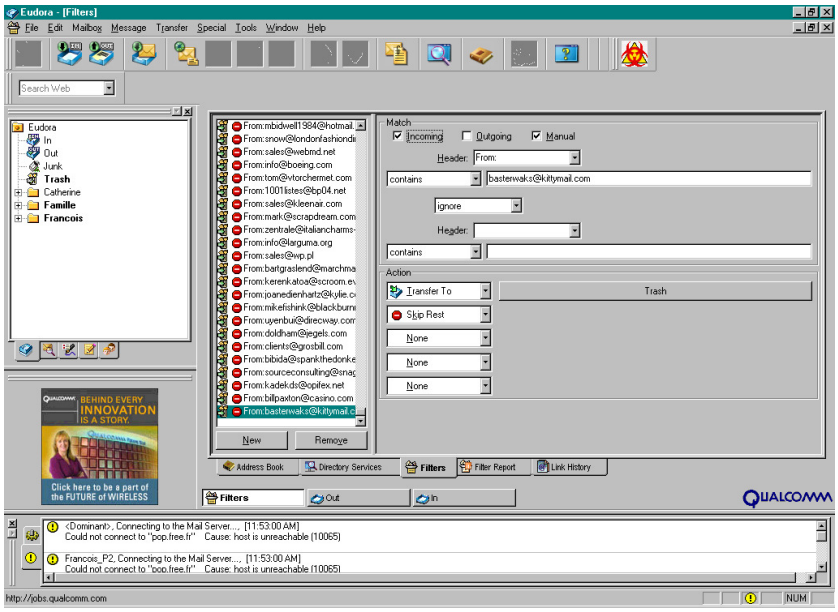
Pour s'en garder, il est possible de :

- *placer des filtres sur sa messagerie* : les logiciels de messagerie offrent ces fonctions et en général, ça suffit
- *utiliser des fonctions anti-spam* si votre PAI en propose[60]
- *utiliser un logiciel spécialisé* :
  - *Mailwasher*, à : http://www.mailwasher.net/
  - *SpamPal*, à http://www.spampal.org/

Des filtres sur sa messagerie

Par exemple, avec Eudora, une liste des filtres existants :

[60] voir plus loin



Dans cet exemple, environ 24*45= 1080 filtres différents existaient au moment de la capture d'écran présentée ici.

Remarques :

- l'élimination d'un message par un filtre est :
  - invisible au destinataire, le plus souvent[61]
  - inconnu à l'expéditeur

L'anti-spam chez Free

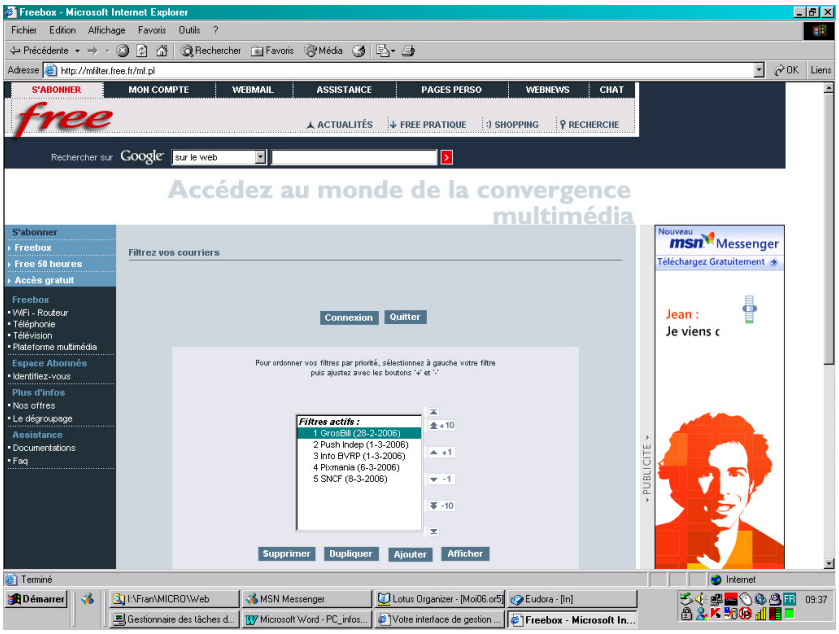
Free propose[62] deux services anti-spam :

- *« système de filtrage des boites aux lettres »*
- *« anti-spam (système …) »*

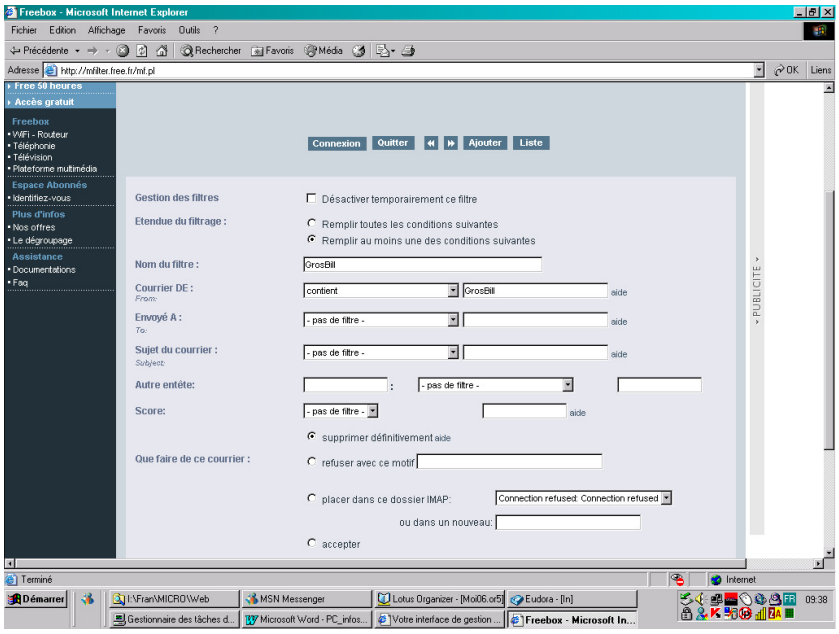
Premier service Free

Le premier service permet de spécifier des filtres spécifiques :

[61] en fonction des options choisies, consistant le plus souvent à mettre à la poubelle le message filtré
[62] depuis Juin 2005

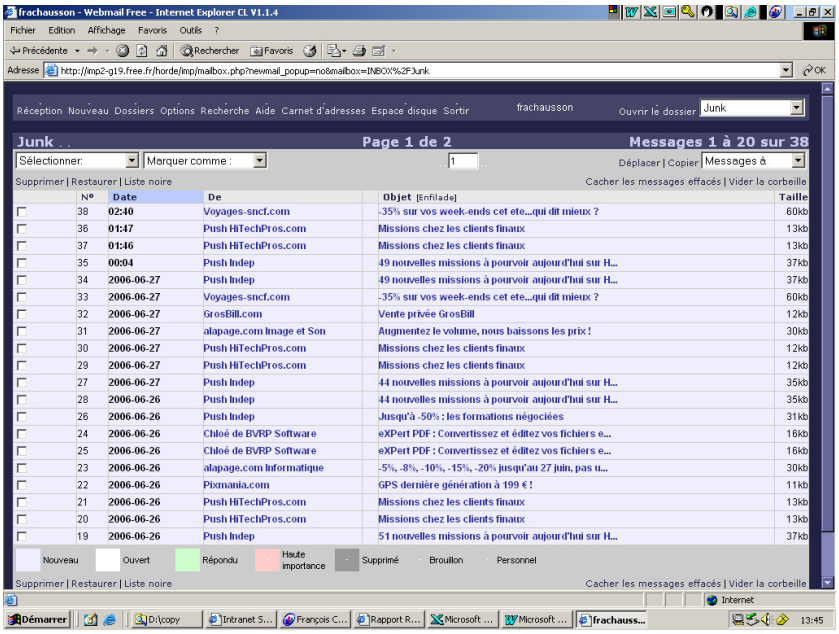


Un exemple de filtre :



Spécifier un / des critère de sélection et de traitement du mail indésirable.

Un exemple du résultat de filtrage :



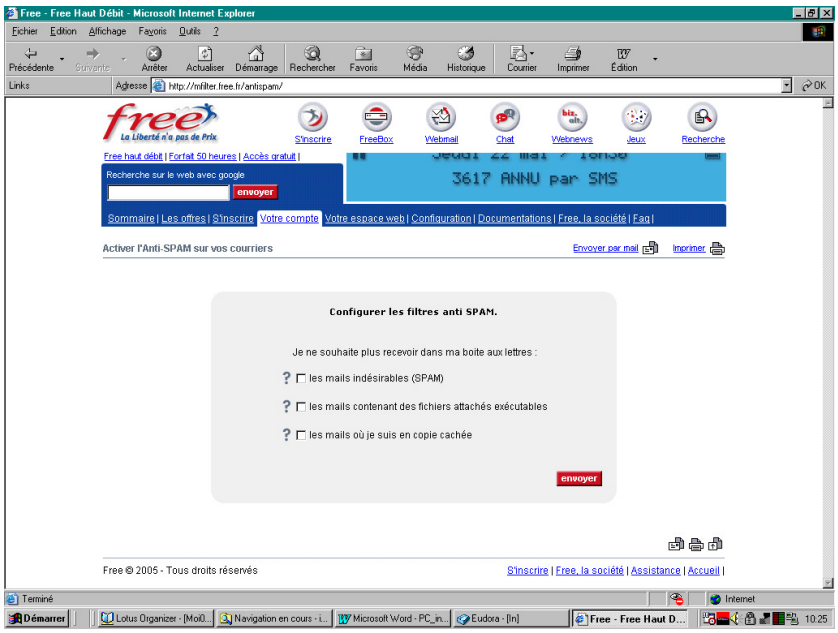
Ici, dans ce dossier *Junk*, se trouvent 38 messages dont 4 du jour.

Remarques :

- ce service de filtrage du PAI n'émet pas de message pour informer de son déclenchement sur un message
- penser ddonc à aller consulter le(s) dossier(s) de messages filtrés pour s'assurer que les filtres ne sont pas trop exigeants en « jettant » des messages qui devraient apparaître dans la Corbeille IN

Deuxième service Free

Le deuxième permet de spécifier des options générales :



Remarques :

- même remarque que précédemment

Une démarche

Il paraît de bonne pratique de mettre en œuvre des mesures anti-spam suivant cette démarche :

- pour les adresses mails relevées par un logiciel de messagerie[63] :
  utiliser de préférence les fonctions de filtrage du logiciel
- pour les adresses mails relevées par Internet Explorer en allant sur le site du serveur
  utiliser les fonctions de filtrage proposées par le PAI

Un filtrage par authentification d el'expéditeur

Des sites proposent un filtrage par identification de l'expéditeur qui élimine à coup sûr tous les messages envoyés par des robots.

Par exemple :

- http://mailinblack.com/

« L'originalité et la performance de MailInBlack résident dans l'authentification de l'expéditeur : lorsqu'un email est envoyé pour la première fois, il est demandé à l'expéditeur de s'authentifier, prouvant ainsi qu'il n'est pas un robot spammeur. Une fois cette procédure simple et rapide effectuée, le message est acheminé au destinataire. Ce principe est imparable. Par ailleurs, tout email porteur de virus est aussi stoppé.

Il est possible de pré-autoriser des expéditeurs déjà connus (qui n'auront pas à s'authentifier) : soit par adresse individuelle, par carnet d'adresses, ou par nom de domaine (utile pour les collègues de la même entreprise ou les newsletters). Pour ces personnes, leurs messages seront transmis automatiquement.

- Par ailleurs, il est possible de bannir un expéditeur importunant, en stoppant systématiquement ses messages, même s'il s'est authentifié »

Les difficultés de l'anti-spam

[63] Outlook, Eudora, …

La lutte contre le Spam peut aussi être trop efficace et supprimer la réception de messages légitimes.

Mes expériences :

- sur mon adresse professionnelle[64], je ne recevais plus des messages légitimes et l'expéditeur n'en était pas averti[65] : les filtres de Free faisaient le travail[66]

Des services anti-spam

Certains PAI font appel, en amont,, à des services anti-spam[67], comme celui fourni par *Spews*[68].

Le critère d'identification du spammer utilisé par Spews est l'adresse IP du serveur du destinataire, autrement dit de votre PAI ; autant dire que tout PAI doit pouvoir se retrouver là très vite car un de ses nombreux abonnés a pu un jour être identifié comme spammer.

Mes expériences :

- les messages d'un correspondant abonné chez Tiscali, un site qui fait manifestement appel à Spews, étaient/sont rejetés[69] et l'expéditeur en était heureusement prévenu[70]

Comment un spammeur identie t il une adresse mail ?

Plusieurs moyens sont utilisés :

- *fourniture volontaire*
- *envoi systématique*
- *« pêche » dans les Forums*
- *avec un nom de site Web*

Leur connaissance permet de limiter les Spams.

Fourniture volontaire

L'adresse mail est souvent demandée à l'internaute :

- achats en ligne : micro informatique, spectacles, …
- …

Recommandation :

-

Envoi systématique

De toute évidence, des spammeurs essayent l'envoi en masse sur des adresses simples :

- a@free.fr[72], b@free.fr, c@free.fr, …
- aa@free.fr, ab@free.fr, …
- aaa@free.fr, …

---

[64] un moment filtrée par Free (par erreur), en plus de l'être par Eudora
[65] c'est ce qu'on peut faire de pire
[66] sans fournir d'information, ce qui est juste normal
[67] depuis début 2005
[68] http://spews.org
[69] = je ne les recevais pas
[70] et m'en a informé
[71] ou un autre PAI
[72] ou un autre PAI

Recommandation :

- ne pas choisir une adresse trop courte

« Pêche » dans les Forums

Les adresses mail laissées dans les Forum sont publiques.

Un spammeur peut simplement draguer les Forums et récupérer ces adresses.

Recommandation :

- dans les Forums, utiliser une adresse mail spécialisée

Avec un nom de site Web

Un propriétaire de site Web peut se faire adresser du courrier en utilisant le nom de domaine.

Par exemple :

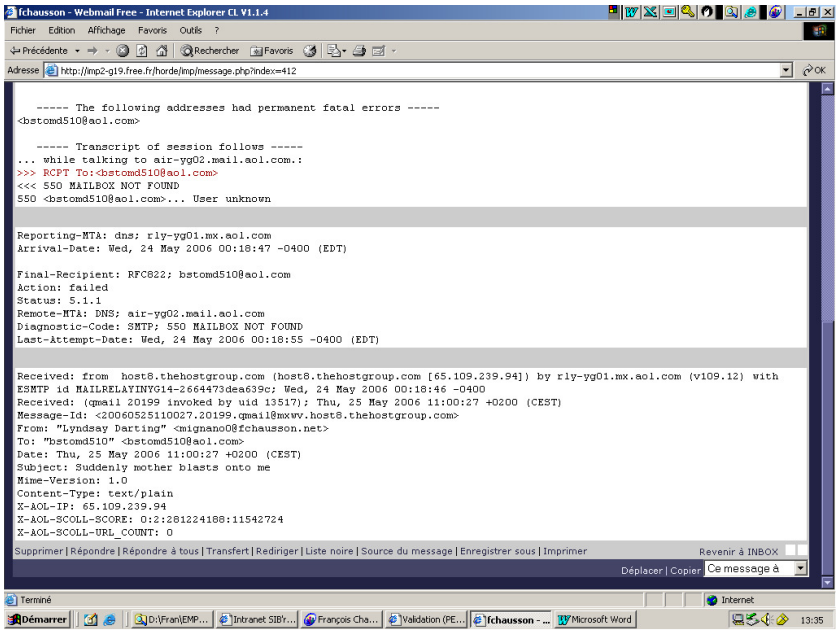
- propriétaire de www.montruc.net
- peut se faire adresser du courrier sur nimportequoi@montruc.net

Recommandation :

- ne pas utiliser cette possibilité

L'usurpation d'identité

Un cousin du Spam : des mails sont envoyés par des individus non identifiés sous une adresse de messagerie vous appartenant, par exemple :



L'expéditeur a donc usurpé votre identité de messagerie pour envoyer un message.

Vous n'en êtes informé que si le message est rejeté en erreur par son destinataire.

La messagerie de La Poste

La Poste fournit gratuitement à tout demandeur une adresse de messagerie électronique dans le cadre de son service public.

L'accès

L'accès à cette messagerie se fait par le site Web de La Poste exclusivement[73].

Comment s'y prendre ?

Pour en bénéficier, il faut dans l'ordre :

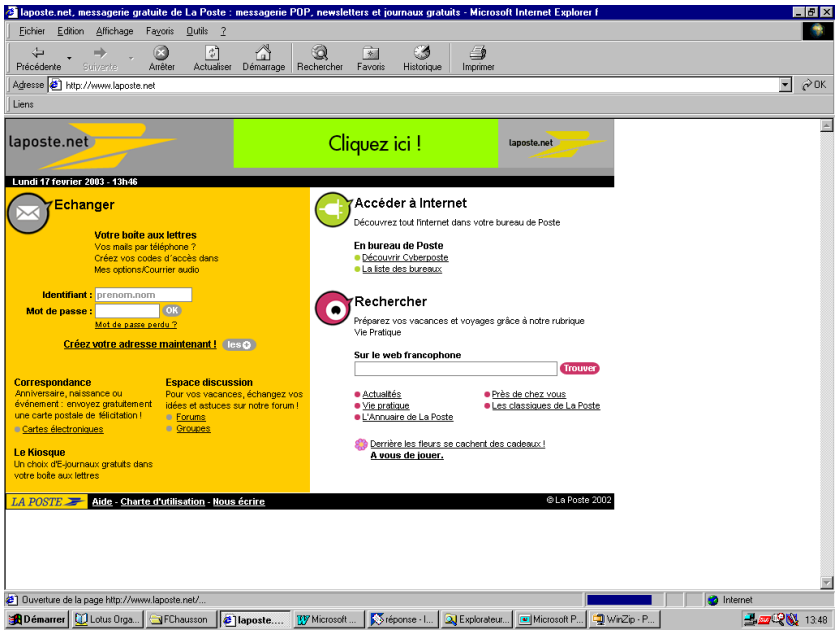
- *Créer son adresse de messagerie,* p. 30
- *Accéder à la* messagerie*,* p. 31

Créer son adresse de messagerie

Avec son navigateur aller sur le site :

www.laposte.net

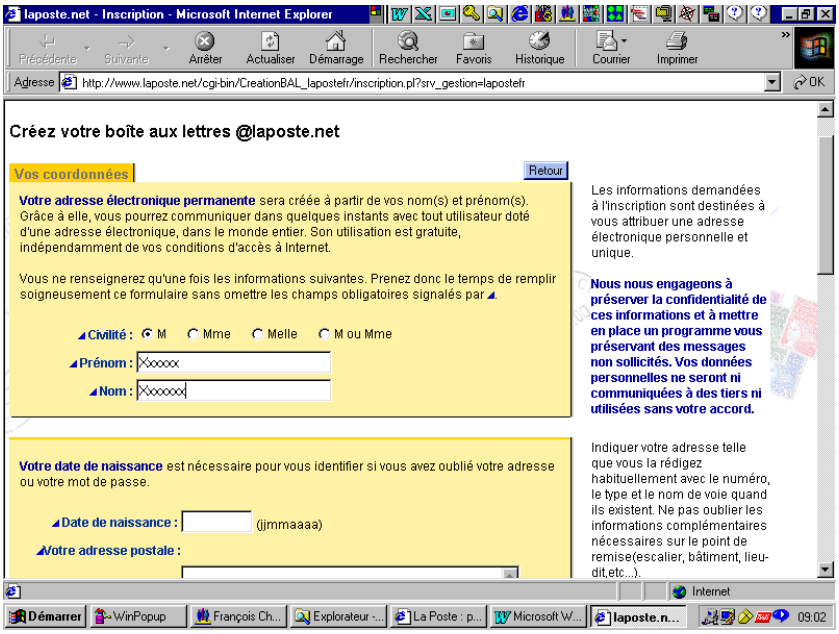
comme montré ci dessous dans le champ Adresse, en haut à gauche[74] :



Cliquer sur la ligne « *Créez votre adresse maintenant* », ce qui amène l'écran suivant :

[73] il n'est pas possible de faire de messagerie à La Poste avec Eudora ou Outlook

[74] Ça, c'est le résultat de la requête mais l'adresse est valide



Remplir tout[75] le formulaire électronique[76] et cliquer à la fin sur « Valider », ce qui provoque l'envoi du formulaire et l'enregistrement de la demande à La Poste.

L'adresse électronique est fournie immédiatement.

Elle est composée sous ce format *prénom.nom*@laposte.net[77] pour autant que ce couple prénom.nom n'y existe pas déjà ; sinon, il y aura un suffixe ajouté.

Un courrier papier de La Poste arrive quelques jours plus tard à l'adresse indiquée dans la demande pour confirmer l'inscription et mentionner toutes les données saisies[78].

Accéder à la messagerie

Une fois l'adresse créée, il est naturellement possible de :

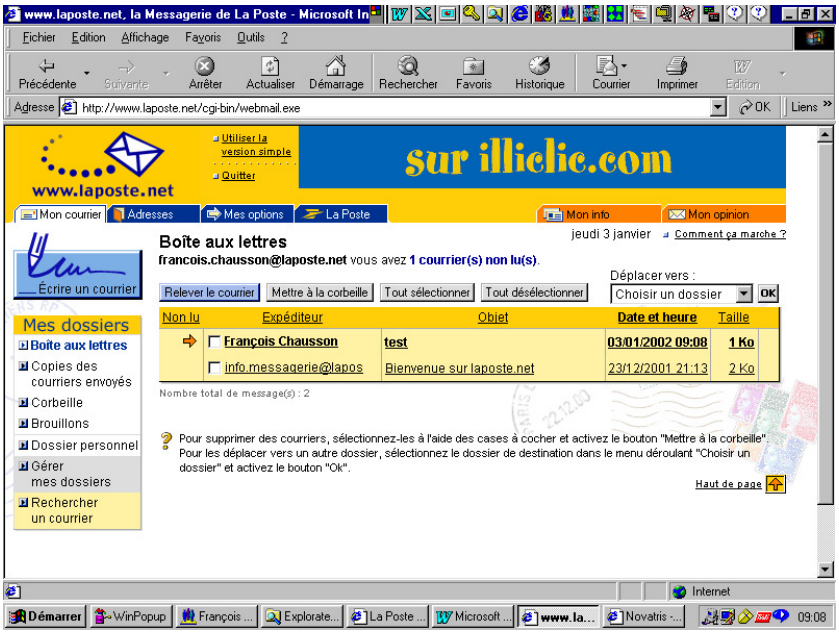
- *Envoyer un message*
- *Recevoir un message*

Envoyer un message

- se connecter avec son navigateur au même site La Poste
- saisir dans les deux cases présentées l'identifiant *prénom.nom*[79] puis le mot de passe en dessous

La liste des messages en attente s'affiche sur un écran comme celui-ci :

[75] c'est un peu long
[76] à un moment, il demande, fort justement, le nom de la grand-mère du futur utilisateur
[77] exemple : francois.chausson@laposte.net
[78] même le mot de passe, ce qui est un peu étrange
[79] ne pas ajouter @laposte.net, le système le fait lui-même et, de plus, ne supporte pas qu'on le fasse à sa place



où il est possible de créer/envoyer des messages, de les lire, de les supprimer, etc…

Recevoir un message

Tout correspondant utilise son logiciel habituel de messagerie pour envoyer un message à l'adresse de l'utilisateur *prénom.nom*@laposte.net.

Attention :
Ces messages arrivés au site La Poste[80] ne seront "vus" par le destinataire que quand il ira consulter sa boite aux lettres[81] ; il faut donc avertir le destinataire s'il n'y va pas voir régulièrement.

Dit autrement, dans cette formule de messagerie, rien ne prévient un destinataire de l'arrivée d'un message.

La messagerie de Free

La démarche est naturellement très semblable à celle suivie pour La Poste.

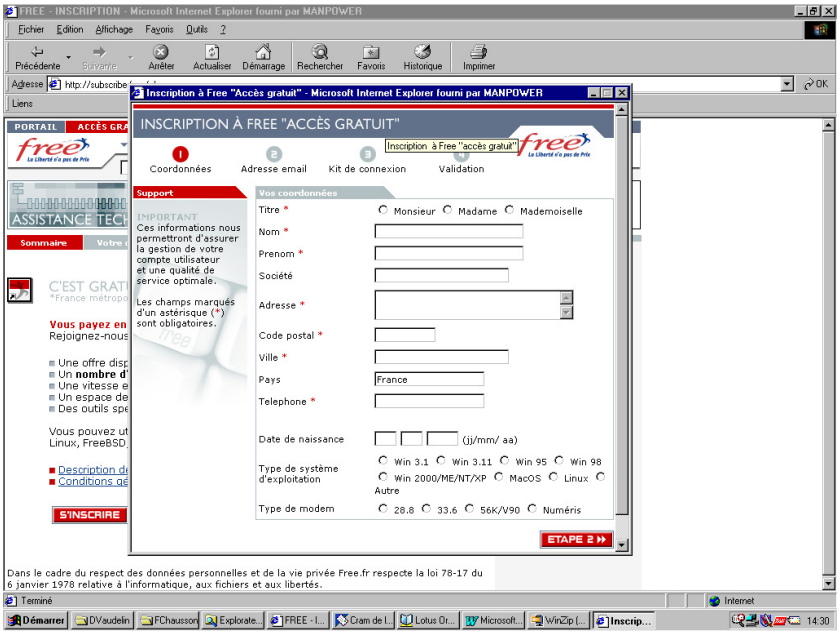
Demande de création d'un nouveau User

- Se connecter à http://www.free.fr

[80] de manière générale, chez tous les PAI pour lesquels il faut aller sur leur site Web pour faire de la messagerie
[81] de manière analogue au service de poste restante pour le courrier papier

- Cliquer sur « Accès gratuit »

- Cliquer sur « S'inscrire »
- Remplir le questionnaire :



Deux modes de connexion

Avec :

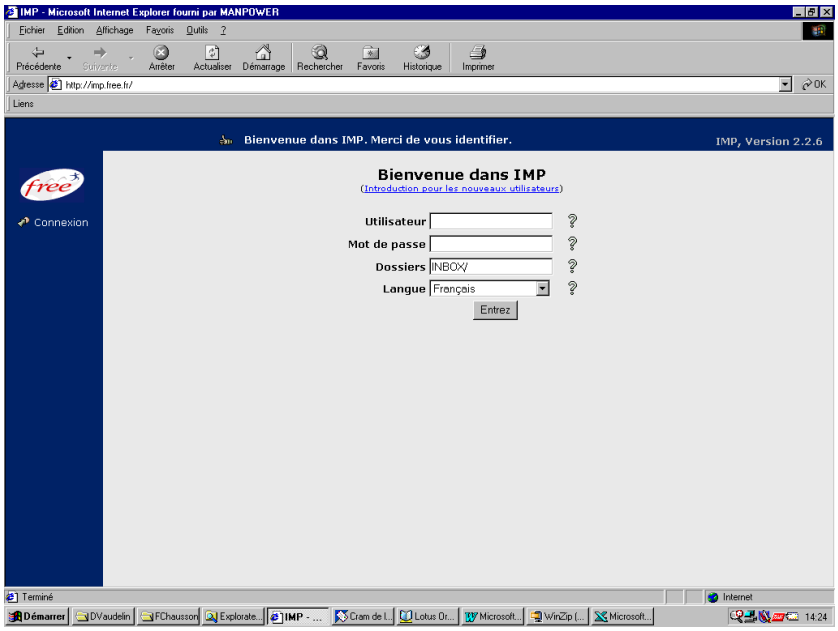
- le user, défini à l'inscription
- le mot de passe, reçu par le courrier

Connexion à la messagerie par son logiciel de messagerie

- Installer le kit demandé lors de l'inscription

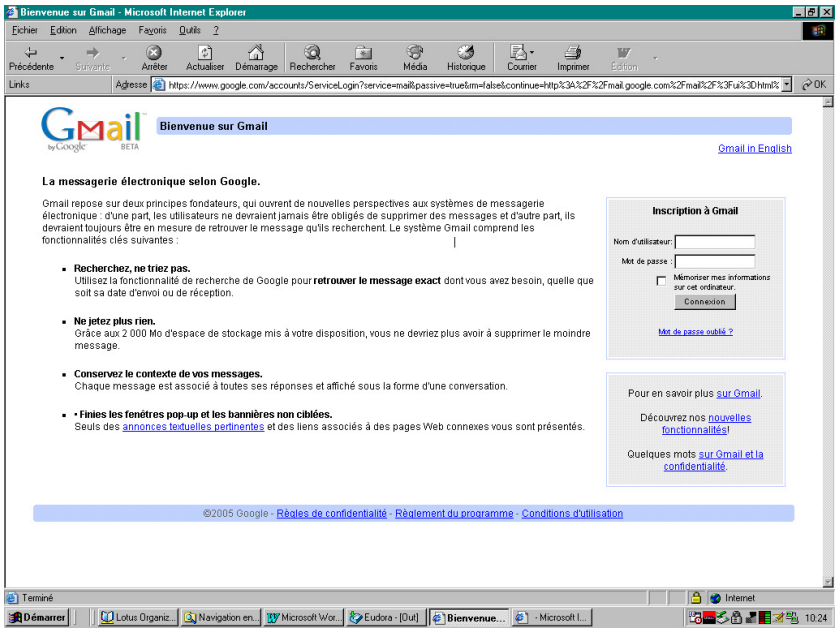
Connexion à la messagerie par le site Free

- Se connecter à http://www.free.fr
- Cliquer sur « Webmail »



La messagerie de Google

Encore en test en Août 2005 :



Protocoles de messagerie

Les échanges de messagerie s'appuient sur deux protocoles différents suivant le sens de l'échange.

Protocol SMTP

- SMTP : Simple Mail Transfer Protocol
- Utilisé pour transmettre le mail depuis l'émetteur jusqu'au serveur du destinataire

Protocole POP3

- POP : Post Office Protocol
- Utilisé pour aller rechercher ses mails sur un serveur
- Nécessite une connexion en TCP/IP, accès par le port 110
- Peut être utilisé avec ou sans SMTP
- Un protocole plus récent d'usage identique : IMAP (Internet Message Access Protocol)

Dans le paramétrage initial d'un logiciel de messagerie[82], il faut donc spécifier deux serveurs.

[82] comme Outlook, Eudora, …

Une adresse de messagerie pérenne

Besoin

Une adresse de messagerie courante contient une référence physique au prestataire :

- le nom technique du prestataire d'accès : *wanadoo, easyconnect, noos, …*
- le nom technique de l'employeur : *deloitte, c3if, manpower, …*
- …

Ces adresses ne sont pas pérennes puisqu'elles changent à chaque « déménagement », soit professionnel, soit privé, forçant ainsi à informer ses correspondants du changement et perdant ceux qu'on oublie.

Moyen

Plutôt que d'utiliser une adresse « physique », il faut disposer d'une adresse « logique » pointant en arrière plan sur l'adresse physique du moment.

Erreur! Aucune rubrique spécifiée.

Il est alors facile, lors d'un « déménagement », de modifier uniquement le lien entre « logique » et « physique ».

Remarques :

- ce mécanisme est exactement celui utilisé également pour un site Web en prenant un nom de domaine plutôt que d'utiliser l'adresse physique du site

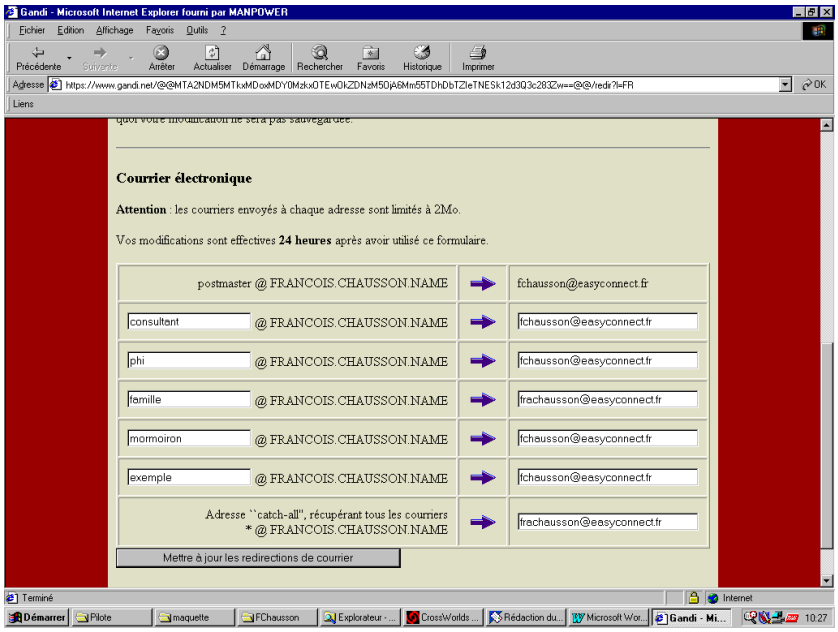
Outil

Il faut utiliser un service de *redirection* d'adresse de messagerie, exactement comme une redirection de site Web[83].

Par exemple, aller chez www.gandi.net et faire :

- *gestion de vos données chez Gandi*
- *Vos redirections Gandi*
- logon sous le user Gandi[84]
- sélectionner le domaine[85]
- spécifier les différentes redirections dans le panneau suivant :

[83] voir le document *PC_infos_Interne 2.doc*
[84] le créer s'il n'existe pas encore
[85] le créer s'il n'existe pas encore



Les redirections peuvent se faire, comme présenté ici, vers différentes adresses[86].

[86] pas forcément vers une seule et même adresse

Se protéger des accès non sollicités ?

La connexion à Internet

A chaque connexion à Internet, le réseau attribue automatiquement[87] une adresse[88] unique dans le réseau et utilisée pour tous les échanges, que ce soit pour les échanges de messagerie ou pour les accès aux sites Web.

Erreur! Aucune rubrique spécifiée.

Le besoin

Il existe différents groupes nuisibles sur le réseau qui essaient, avec des motivations différentes[89], de pénétrer sur les micros connectés en « ciblant » leur adresse Internet[90].

Pour un nuisible, il suffit donc de trouver l'adresse d'un utilisateur connecté pour y entrer sans aucune difficulté, sauf si cet utilisateur a installé une protection adéquate.

Noter aussi, qu'à l'inverse, des logiciels[91] installés sur un micro envoient parfois des informations, vers leur éditeur le plus souvent, qui sont des échanges également bons à contrôler.

Il faut donc contrôler autant les accès *entrants* que les accès *sortants*.

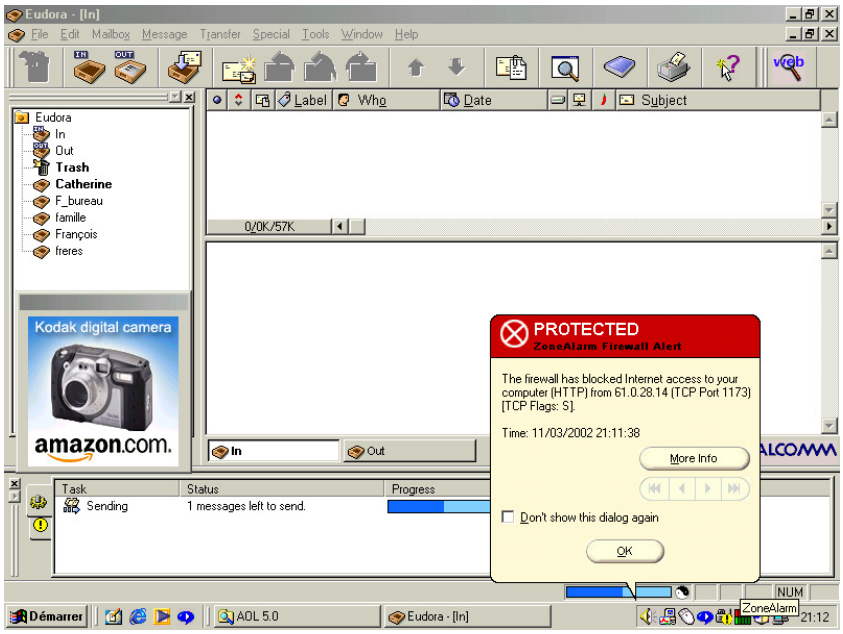
Risque

En l'absence d'un logiciel de protection spécialisé, le risque peut aller jusqu'à retrouver son disque dur complètement effacé, en passant aussi par le dépôt direct d'un virus[92].

Exemple

Dans cet exemple, une tentative d'intrusion venant de l'adresse IP 61.0.28.14 a été bloquée par un logiciel spécialisé :

[87] l'adresse est attribuée de manière dynamique, parfois différente d'une connexion à l'autre
[88] dite adresse IP
[89] tout l'éventail entre la farce et le ravage
[90] la méthode la plus courante consiste à scanner automatiquement des plages entières d'adresses jusqu'à en trouver une qui soit active
[91] Realplayer, etc …
[92] la protection contre les virus est présentée dans un autre document



Il faut quand même remarquer que de nombreux « hits » proviennent des tests routiniers réalisés par les divers gestionnaires du réseau.

Le moyen

En réponse à ces tentatives, en entrée comme en sortie, la démarche consiste à dresser un « mur » filtrant pour s'y opposer.

C'est le « Firewall », le mur de feu, qui filtre les accès pour autoriser uniquement ceux qu'on estime légitimes.

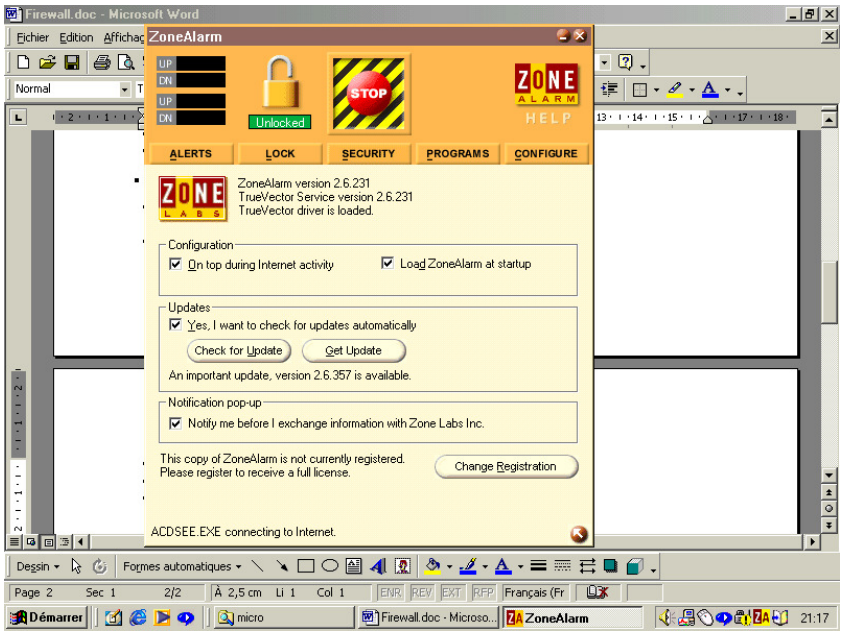
Un logiciel de Firewall

La mise en œuvre

Il est facile en général de spécifier les différents comportements attendus d'un Firewall.

Bien souvent, ces spécifications n'ont pas besoin d'être élaborées à la mise en œuvre mais se construisent à mesure où les situations nouvelles se présentent[93].

[93] ce qui en rend la mise en œuvre aisée



L'outil

Il existe divers logiciels Firewall ; le logiciel **ZoneAlarm**[94] est à la fois reconnu comme un Firewall efficace et apprécié pour sa gratuité pour des usages domestiques.

Il est possible de le télécharger depuis :

- www.tucows.com
- http://www.zonelabs.com/store/content/company/products/trial_zaFamily/trial_zaFamily.jsp?lid=zassskulist_trial

D'autres firewall :

- le Firewall de Windowsz XP : ne filtre que les entrées, pas les sorties[95]
- www.kerio.com
- www.tinysoftware.com
- soho.sygate.com/free
- www.agitum.com

Trucs et astuces

Quand une installation comprend plusieurs micros reliés par un réseau local et qu'une connexion Internet doit être mise en œuvre, il faut suivre cette règle :

- *pas de double connexion*

Autrement dit, le poste qui est connecté à Internet ne doit pas être connecté au réseau local[96] ; c'est la meilleure manière d'instaurer une protection totalement efficace en séparant physiquement les deux mondes, Internet et réseau local.

[94] voir Zone Alarm en annexe
[95] un certain nombre de logiciels (RealPlayer, …) émettent vers leur éditeur à l'insu de l'utilisateur sans Firewall filtrant les sorties
[96] et réciproquement

Notice d'utilisation

Consulter le document *Utiliser Zone Alarm*.

Sécurité et Internet

La sécurité sur Internet est gérée par différents acteurs :

- *Internet Explorer*
- *Les Firewall*
- …[97]

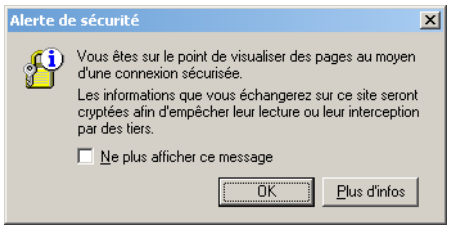
Sécurité et Internet Explorer

Internet Explorer gère plusieurs situations de sécurité :

- *Sécurisation des échanges*
- *Niveaux de sécurité des zones*

Echanges sécurisés

En accédant à un site Web sécurisé[98], celui-ci envoie automatiquement une information :



Voici un exemple d'accès à un site sécurisé :

Deux points importants sont à noter :

- quand une connexion est sécurisée, l'URL du site visité commence par HTTPS[99]
- Internet Explorer affiche une icône représentant un verrou sur la barre d'état[100]

---

[97] Les « antis » : anti virus, anti spyware, …
[98] Sécurisation : par SSL
[99] le *S* signifie que le *protocole SSL* est en action

Le protocole SSL :

- identifie le serveur en vérifiant qu'il détient bien un certificat délivré par une autorité reconnue
- il fournit au Client[101] et au Serveur la possibilité de sécuriser leurs échanges en les cryptant

Un certificat est une mention garantissant l'identité d'une personne ou la sécurité d'un site Web ; voir plus loin des informations sur les certificats.

Voir plus loin les informations concernant le *Phishing*.

Stratégie de sécurité personnelle

Si un besoin de vérification apparaît, vérifier :

- le contenu de la page : logo, mise en page, …
- l'URL apparaissant dans la barre d'adresse[102] pour s'assurer qu'elle n'a pas changé en cours d'interrogation, au moins pour sa partie racine
- que l'URL commence par HTTPS
- la présence du verrou au bon endroit

Zones Internet et niveaux de sécurité

Zones Internet de IE

IE définit 4 zones distinctes :

Erreur! Liaison incorrecte.

auxquelles il affecte des niveaux de sécurité différents

- zone *Intranet local* : niveau de sécurité *Moyen*
- zone *Sites de confiance* : niveau de sécurité *Faible*
- zone *Internet* : niveau de sécurité *Moyen*
- zone *Sites sensibles* : niveau de sécurité *Haut*

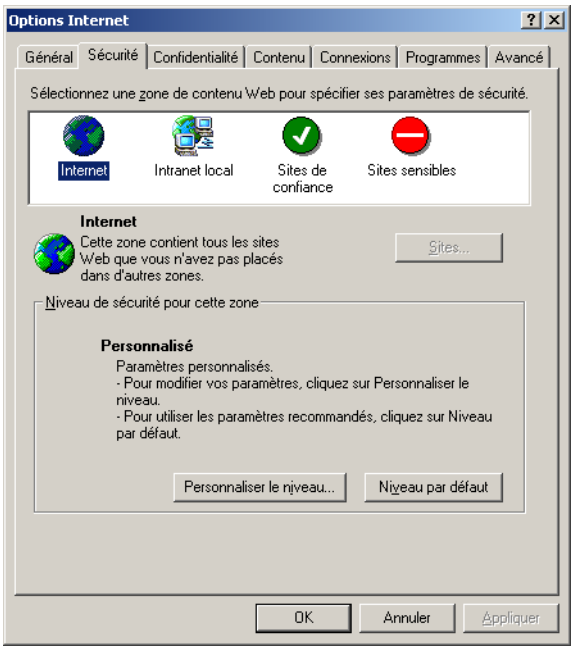
Niveaux de sécurité de IE

IE décrit un niveau de sécurité pour chaque zone :

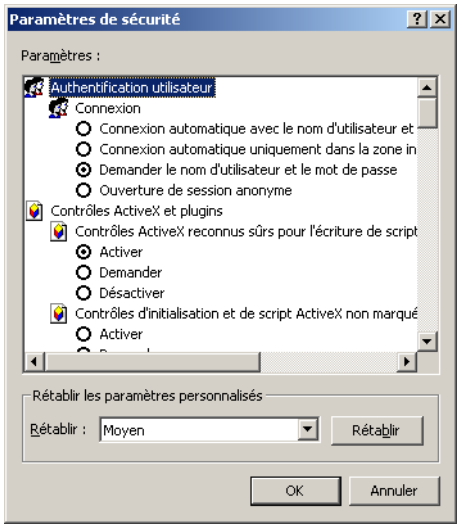
[100] attention : cet affichage :
- apparaît dans la barre d'état de IE, en bas, et non pas dans la page visualisée
- ne se produit que lorsque la connexion a besoin d'être sécurisée, et non pas de manière permanente

[101] Client : vous, moi, …

[102] au besoin, ouvrir une nouvelle fenêtre et saisir l'URL du site choisi à la main



Chaque niveau de sécurité[103] est décrit en détail :



et tout peut être modifié.

Sécurité et Firewall

La logique générale d'un Firewall est de ne laisser entrer / sortir que les accès autorisés.

Le Firewall WinXP

Le Firewall WinXP contrôle les flux entrants uniquement.

Ce Firewall est :

- Partie intégrante de WinXP
- En service par défaut

[103] Ici, la zone *Internet*

Par ailleurs, il ne pose pas de questions à l'utilisateur, gérant les situations en accord avec ses paramétrages.

Le Firewall ZoneAlarm

Le Firewall ZoneAlarm contrôle les flux entrants et sortants.

Ce Firewall est :

- Un logiciel indépendant de WinXP
- A installer / paramétrer

Ce Firewall est assez bavard, pose des questions à l'utilisateur pour compléter ses paramétrages et requiert une bonne compréhension du fonctionnement d'un micro et de l'Internet.

Les Zones de ZA

ZA définit deux zones :

- *Trusted zone*
- *Internet zone*

La *Trusted zone* est destinée à abriter les sites de confiance en laissant les accès se réaliser conformément aux règles de sécurité de ce groupe.

Le Firewall de la Livebox

La Livebox de Wanadoo embarque un firewall qui est activé par défaut.

Un peu comme le FW WinXP, il ne dit rien.

Firewall et routeur, un empilement ?

Quand un réseau local (WiFi), est connecté à Internet par un routeur, la protection contre les intrus est déjà bien assurée.

En effet, tant qu'un port n'est pas Forwardé, personne ne pourra pénétrer sur un des postes du réseau local.

Limitations

Dans cette configuration, la mise en œuvre d'un Firewall présente quand même plusieurs atouts :

- Un firewall peut contrôler les flux sortants du micro[104]
- Un firewall protège d'une éventuelle intrusion dans le WiFi directement

[104] Pas le firewall WinXP

Supprimer les intrus et se garder des importuns

Au delà des agressions par les virus[105], du Spam[106] et des attaques directes lors de connexions Internet[107], il existent d'autres populations de nuisibles :

- *les Spywares*
- *les Hijackers*
- *les Hoax*
- *le Phishing*
- *les Rootkits*
- *les Dialers*
- *les Key loggers*

Les Spywares

Ckoiça ?[108]

De nombreux logiciels proposés sans facturation intègrent légitimement des démarches publicitaires fournies par des sociétés qui, en échange, paient donc pour le logiciel, son développement d'abord puis sa maintenance.

La logique générale est : « Vous utilisez mon logiciel gratuitement, alors vous regardez ma pub » ; là, nous ne sommes arrivés qu'au *Adware* : Advertising supported software.

Simplement, il est fréquent que ces logiciels incorporent aussi des fonctions de collecte d'information, sans forcément respecter les réglementations sur la confidentialité des données[109] et souvent sans le dire à l'utilisateur ; ces informations concernent particulièrement les habitudes de surf et sont transmises discrètement à la société intéressée, celle qui a payé pour avoir ces données.

Nous sommes bien arrivés maintenant au *Spyware*, un objet qu'il est important d'identifier, au minimum, et parfois de supprimer.

Le Spyware est donc un espion mais en aucune manière un destructeur comme un virus.

Que faire?

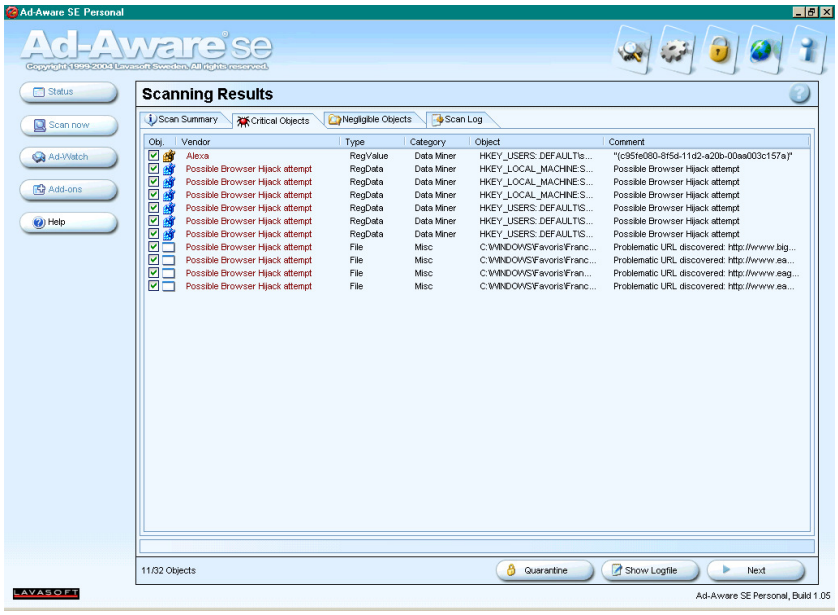
Leur suppression peut être effectuée à l'aide d'un logiciel spécialisé comme :

- *Ad-Aware*[110] à http://www.lavasoftusa.com/
- *Spybot* à xxx
- *SpywareBlaster*
- *SpyHunter*

Par exemple, avec Ad-Aware :

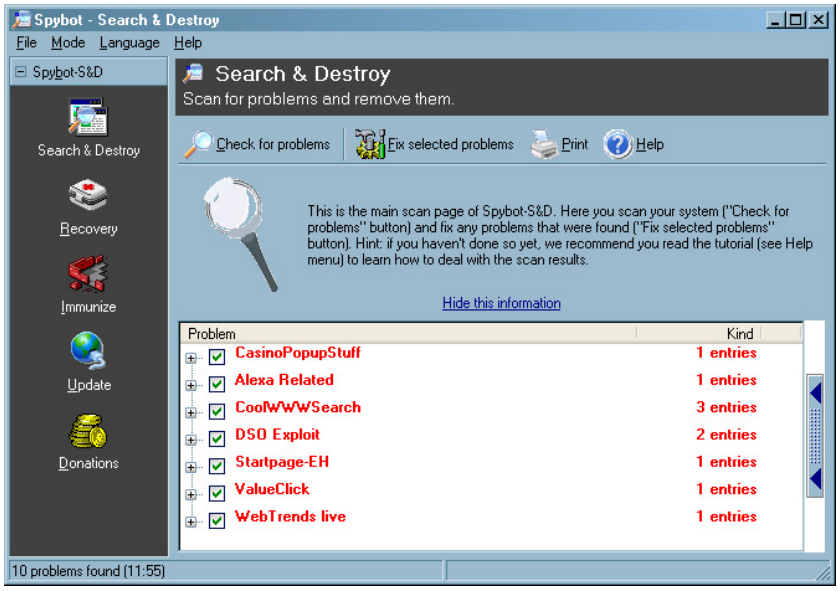
---

[105] voir le document *PC_infos_micro1.doc*
[106] tous les e-mail non sollicités
[107] prises en charge par un *Firewall*
[108] « C'est quoi ça ? »
[109] un concept éminemment variable suivant les pays, les époques, …
[110] voir le document « Micro-ordinateurs, informations, idées, trucs et astuces, Utiliser AdAware ».



Voici 11 objets suspects détectés par Ad-Aware.

Par exemple, avec Spybot :



Remarques :

- Beaucoup ne voient pas de différence réelle entre un virus et un spyware

Les espions XP

Dans la catégorie Espion, Windows XP héberge plusieurs fonctions dont le rôle consiste à envoyer à Microsoft des informations.

Pour supprimer ces envois, il suffit de mettre en œuvre un logiciel comme :

- *XP Anti spy* : un Freeware, à charger sur le site du même nom

Les Hijackers[111]

Ckoiça ?

Des parasites de type divers peuvent être « accrochés » à Internet Explorer et en modifier le comportement.

Le cas le plus fréquent consiste en un remplacement de page par défaut (front page hijacking) ; certains autres s'attaquent à la barre d'action, aux boutons, etc…

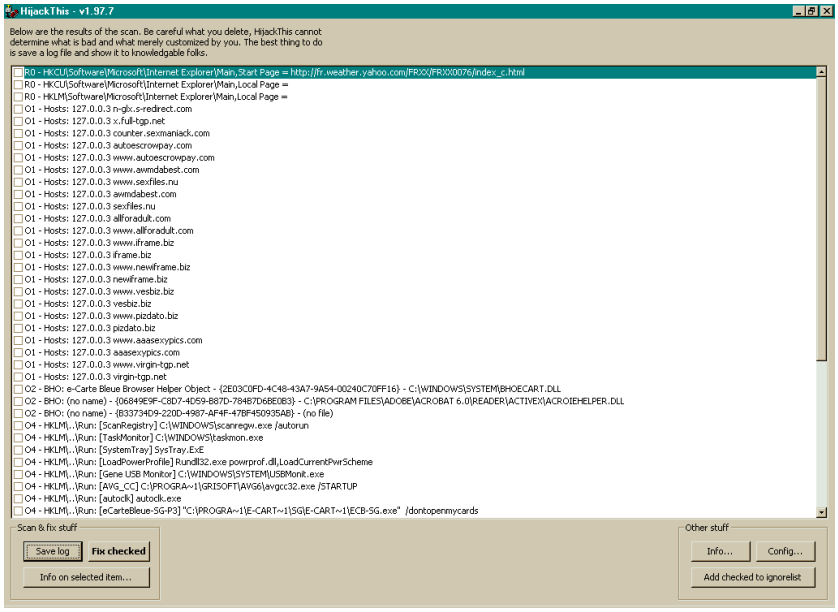
Le Hijacker est le plus souvent une redirection forcée vers un site en particulier mais pas un destructeur comme un virus.

Que faire?

Leur suppression peut être effectuée à l'aide d'un logiciel spécialisé comme :

- *HijackThis*[112]

Par exemple :



Voici une liste des *Bons* et des *Mauvais*, à chacun d'y reconnaître les siens.

Le Hoax

Le *Hoax,* un cousin des virus, est une action qui consiste à propager une information fausse, périmée ou invérifiable au sujet d'un prétendu virus.

L'objectif est de faire supprimer par le destinataire du message un fichier, supposé infecté, dans le système.

Toujours une blague, souvent de mauvais goût, un *Hoax* peut provoquer des dégâts par les actions de pseudo-sécurité qu'il conseille de prendre.

---

[111] en américain : *Browser add-ons*
[112] voir en annexe « HijackThis, interprétation »

Il est possible de vérifier sa nature sur différents sites comme :

- HoaxBuster : http://www.hoaxbuster.com
- HoaxKiller : http://www.hoaxkiller.com

Juste pour voir un Hoax célèbre, faire une recherche[113] sur *Rachel Arlington*.

Le « Phishing »

Ckoiça ?

Le *Phishing*[114] consiste pour un site Web, habilement nommé et présenté, à solliciter des internautes en se faisant passer pour un autre site Web, celui-ci honorablement connu.

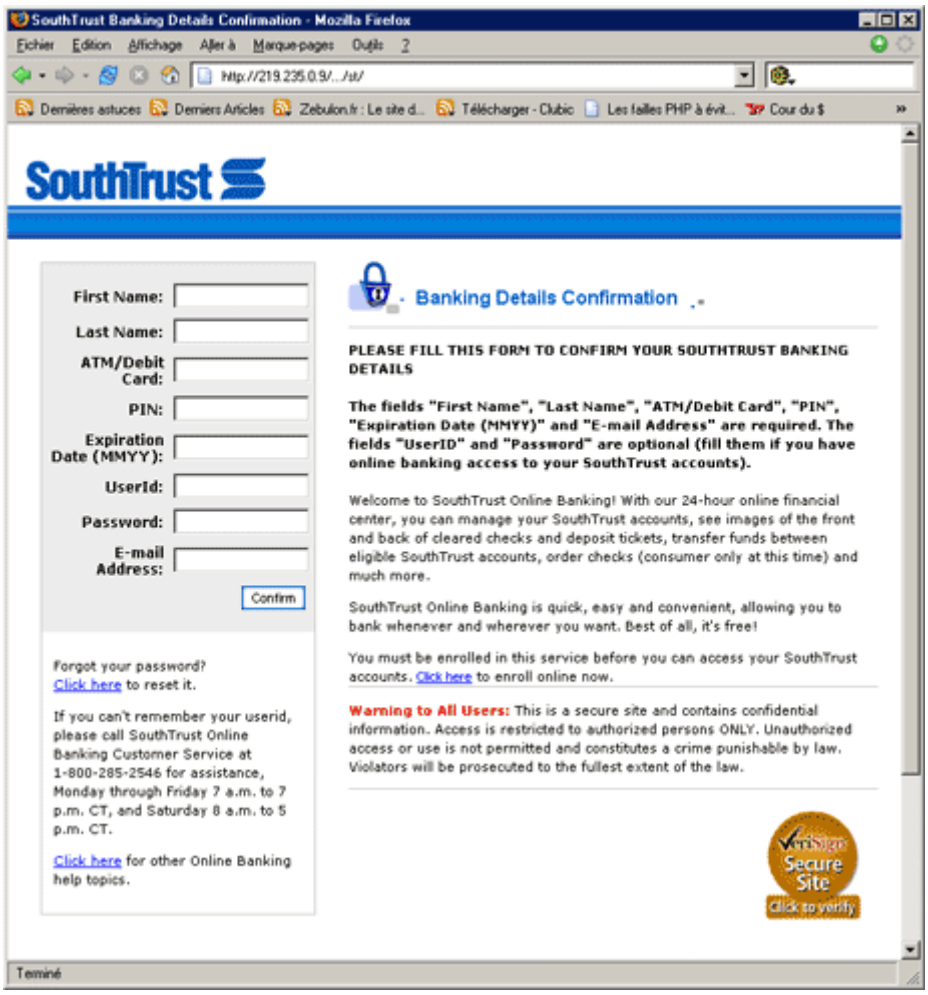
L'objectif est, au minimum de recueillir des informations, le plus souvent d'arriver à réaliser des intrusions dans des comptes bancaires pour les assécher.

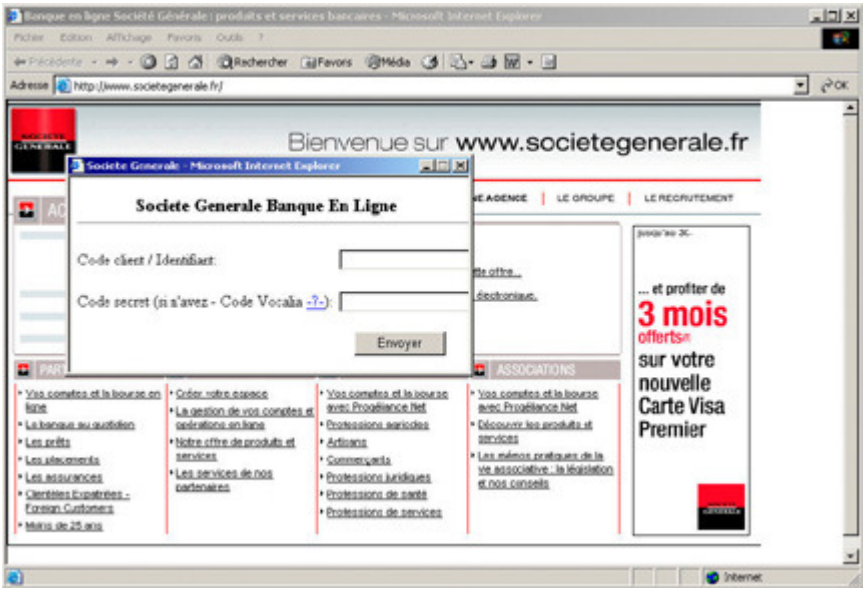
Le Phising peut donc coûter cher en monnaie sonnante et trébuchante.

Des exemples

Voici deux panneaux extraits de deux tentatives de phishing montrant le type de données demandées :

[113] dans Google
[114] si, si, l'orthographe est exacte





Des moyens de détection

Pour commencer, une attention éveillée aux sollicitations extérieures, aux mails surtout, est primordiale.

Différentes démarches sont possibles :

- *Faire quelques vérifications simples*
- *Vérifier l'utilisation d'un protocole d'échange sécurisé*
- *Rechercher le nom de domaine*
- *Utiliser une barre de tâche spécialisée*

Faire quelques vérifications simples

- L'URL du site visité doit commencer par HTTPS
- Internet Explorer doit afficher un petit cadenas jaune dans son bandeau, en bas à droite :

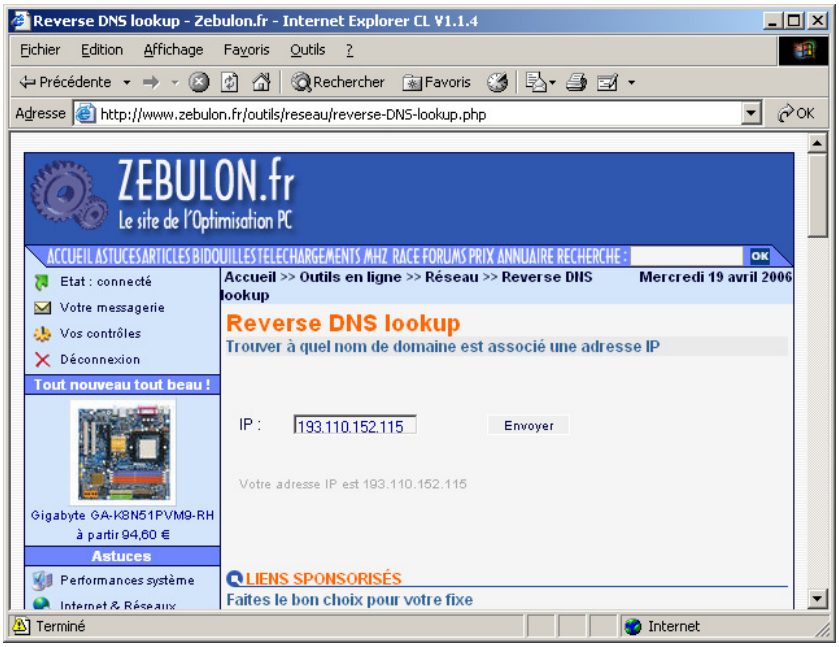
-

Vérifier l'utilisation d'un protocole d'échange sécurisé

Voir la description en annexe.

Rechercher le nom de domaine

Il est possible de rechercher le nom de domaine correspondant à une adresse IP, par un service de *Reverse DNS lookup* comme celui-ci :
http://www.zebulon.fr/outils/reseau/reverse-DNS-lookup.php

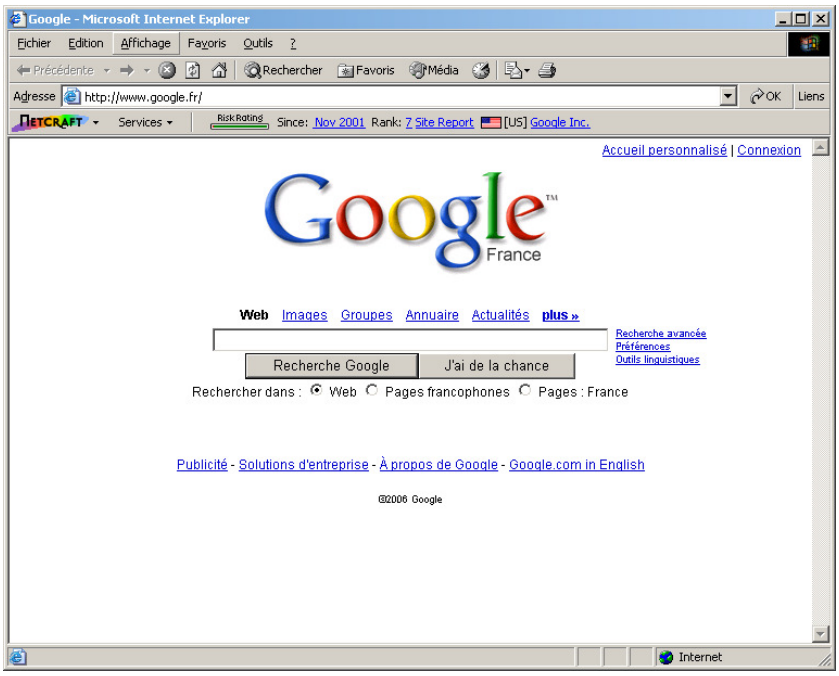


Si le nom de domaine trouvé n'est pas cohérent[115], la fraude est vraisemblable.

Utiliser une barre de tâche spécialisée

Voir sur http://www.zebulon.fr/articles/phishing-4.php

[115] ex. : www.societegenerale.fr



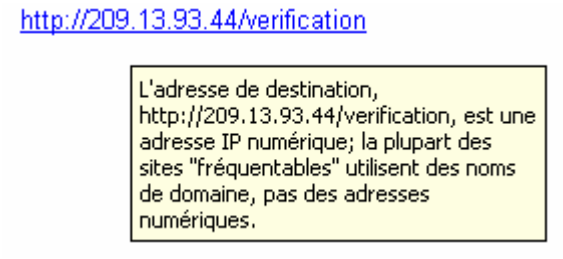
Nous constatons ici que :

- la barre *Risk Rating* (évaluation du risque ou indice de risque) est verte, ce qui signifie que le site est sûr ; l'évaluation du *Risk Rating* se fait selon différents paramètres (localisation géographique du serveur, adresse IP, personne ayant déposé le nom de domaine...)
- date de création du site : les sites de phishing étant très éphémères, une date de création très récente peut être mauvais signe
- rang : il est calculé en fonction du nombre d'utilisateurs de la barre Netcraft qui ont visité le site
- rapport de site : un clic sur le lien "Site Report" affiche de nombreuses informations concernant le site en question comme le DNS et son propriétaire, l'IP du serveur, les différent hébergeurs du site qui se sont succédés ; il est conseillé de se méfier d'un site qui ne propose que peu d'informations
- la nationalité : un petit drapeau indique ici la nationalité du site visité ; cette indication est bien pratique car il y a peu de chance qu'un site d'une banque française soit hébergée en Russie par exemple
- le dernier lien indique quant à lui les différents rapports des sites étant chez le même hébergeur

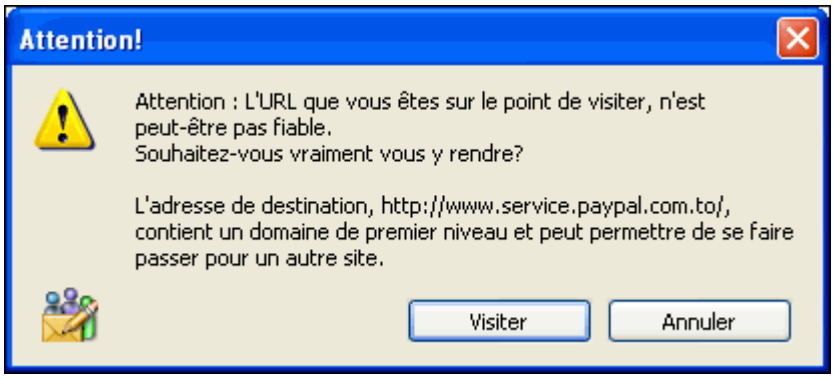
Des moyens de protection

Un logiciel de messagerie comme Eudora propose une fonction *ScamWatch* qui contrôle les liens inclus dans un mail et avertit s'il y a un doute.

Au passage du pointeur de la souris sur un lien, il peut s'ouvrir une feenêtre comme :



Si l'utilisateur clique quand même sur ce lien litigieux, un message tel que celui-ci apparaît :



Les RootKits

Un « rootkit » est un programme ou un ensemble de programmes permettant à un pirate de maintenir dans le temps un accès frauduleux à un système informatique.

Le pré requis du rootkit est une machine « déjà » piratée.

La fonction principale du « rootkit » est de simplifier, voire automatiser, la mise en place d'une ou plusieurs « backdoors ».

L'installation d'un « rootkit » nécessite des droits administrateurs sur la machine, notamment à cause des modification profondes du système qu'il engendre.

A aucun moment un « rootkit » ne permet de s'introduire de manière frauduleuse sur une machine saine.

Le rootkit automatise l'installation d'une porte dérobée ou d'un cheval de Troie.

La discrétion est l'essence même du « rootkit.

Le meilleur moyen de se protéger des rootkit est donc de se prémunir des failles.

Les Dialers

« The Dialer is a piece of software that is downloaded on to the computer. Its job is to disconnect you from the internet, so that when you re-connect it uses its own software to re-connect you. You probably will not notice any change, as the dialer software does its best to emulate your real connection software, but you will notice when you get a big phone bill because The Dialer has been charging your re-connection (and any subsequent

connections) at £1 a minute for example. Hence its name The Dialer - It dials (connects you to) the internet at a higher price”

Les Key loggers

« A Key Logger is a program that, once downloaded, starts logging (writing in to a log file) all the keyboard keys you are pressing. Once your keys have been logged the log file is sent to a computer for analysing”.

Un portail[116]

Un **portail Web** est un site Web qui offre une porte d'entrée unique sur un large panel de ressources et de services (messagerie électronique, forum de discussion, espaces de publication, moteur de recherche) centrés sur un domaine ou une communauté particulière.
Les utilisateurs ont la plupart du temps la possibilité de s'enregistrer à un portail pour s'y connecter ultérieurement et utiliser l'ensemble des services proposés, dont notamment la personnalisation de leur espace de travail, lequel est organisé à l'aide d'élements d'IHM de base: les portlets.
Généralement, chaque fournisseur d'accès à Internet (FAI), possède son propre portail Web.
Pour créer un portail Intranet dans son entreprise il existe un logiciel gratuit et illimité nommé Honolulu, téléchargeable sur le site http://www.pcsoft.fr/honolulu/index.html
Exemples de portails: Yakeo, Yahoo, l'Internaute...

Honolulu

http://www.pcsoft.fr/honolulu/index.html

PHPportal

[116] Par Wikipedia

Un proxy

Le besoin

Un serveur Proxy[117] est une machine faisant fonction *d'intermédiaire* entre Internet et le/les ordinateurs d'un réseau local.

Le plus souvent, il s'agit d'un proxy HTTP[118].

Le moyen

Lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui transmettre sa requête.

Le serveur proxy va alors se connecter au serveur Internet que l'application cliente cherche à joindre et lui transmettre la requête.

Ce serveur Internet va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

Erreur! Aucune rubrique spécifiée.

Le besoin

Le rôle de relais du serveur proxy peut aussi être assuré par un routeur, mais l'un ne remplace pas l'autre.

En effet :

- Un routeur est parfait pour faire la traduction des adresses, se chargeant bien des flux entrants[119]
- Un proxy est parfait pour contrôler les flux sortants, limité toutefois aux types de flux qu'il supporte[120], en particulier pour limiter l'accès à Internet aux utilisateurs autorisés[121]

Les architectures professionnelles mettent en œuvre les deux équipements de cette manière :

- Des postes, sans l'adresse de la passerelle, s'adressant au proxy
- Un proxy, le seul à connaître l'adresse de la passerelle[122]
- Un routeur

D'autres Proxy ?

- Des Public proxy servers : pour accroître le débit d'une connexion
- Des Anonymous proxy servers[123] : pour préserver l'anonymat

---

[117] = serveur mandataire
[118] d'autres : proxy FTP, …
[119] des flux sortants aussi mais sans les contrôler
[120] HTTP, SMTP, POP3, …
[121] Identifiant / mot de passe
[122] éventuellement, le seul à y être connecté
123 Total Net Shield, Secure Tunnel, ProxyWay

- Des Reverse proxy : pour permettre à des utilisateurs externes d'accéder à un site Web interne

Des infos

- http://www.analogx.com/contents/download/network/proxy.htm
- http://www.commentcamarche.net/lan/proxy.php3
- http://www.publicproxyservers.com/index.html

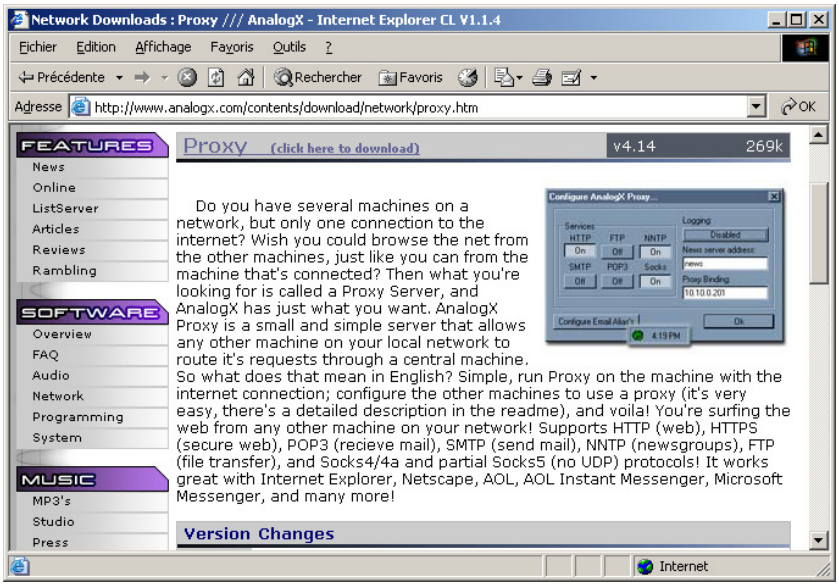
L'outil

Plusieurs logiciels existent sur le marché :

- *Squid* : le plus populaire
- *Wingate*
- *AnalogX*
- *WinProxy*
- Dans Windows 2000, *Microsoft Proxy Server (MSP)*
- …

Un exemple

avec *AnalogX*[124] :



Le principe

Quand un poste secondaire manifeste son besoin d'accéder à Internet, au travers de la connexion commutée du poste principal, si cette connexion n'est pas établie, le proxy en provoque l'établissement.

La déconnexion intervient à l'issue d'un délai d'inactivité paramétrable dans le proxy.

[124] http://www.analogx.com/contents/news.htm

Mise en œuvre

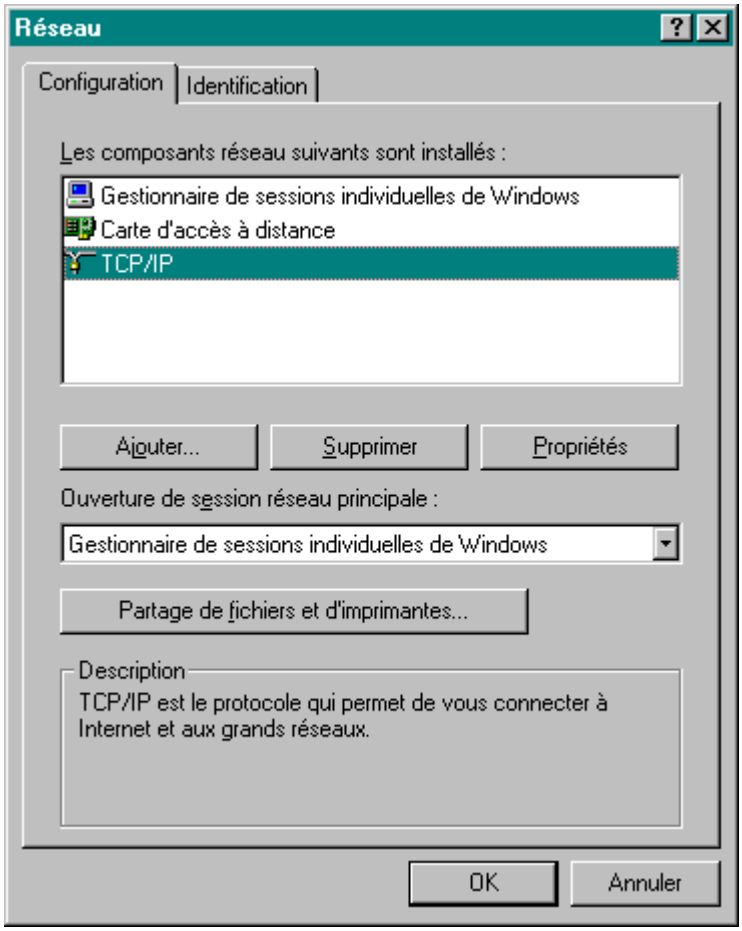
Le poste principal

Sur le poste principal[125], celui qui a la connexion Internet, il faut :

- *vérifier que TCP/IP est activé*
- *choisir une adresse IP pour le Proxy*
- *spécifier le port*
- *installer le logiciel proxy*

Vérifier que TCP/IP est activé

Faire *Démarrer/Paramètres/Panneau de configuration/Réseau*



- TCP/IP apparaît bien dans la liste

Remarques :

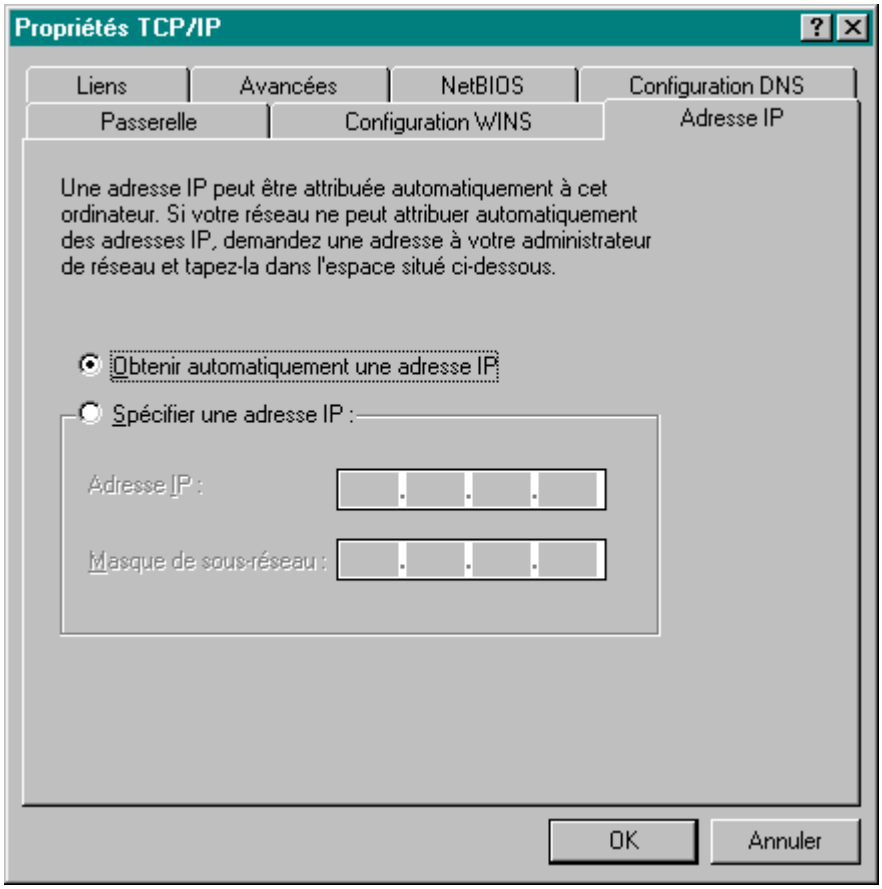
- cette configuration TCP pour le proxy « doublonne » avec la configuration TCP existante pour la connexion Internet ; si, à la création de la configuration TCP pour le proxy, celle-ci était « accrochée » à la connexion Internet, il faudrait supprimer les deux configurations, créer celle pour le proxy avant de créer celle pour la connexion Internet

Choisir une adresse IP

Sur la connexion avec le/les autres postes[126], il faut assigner une adresse au proxy :

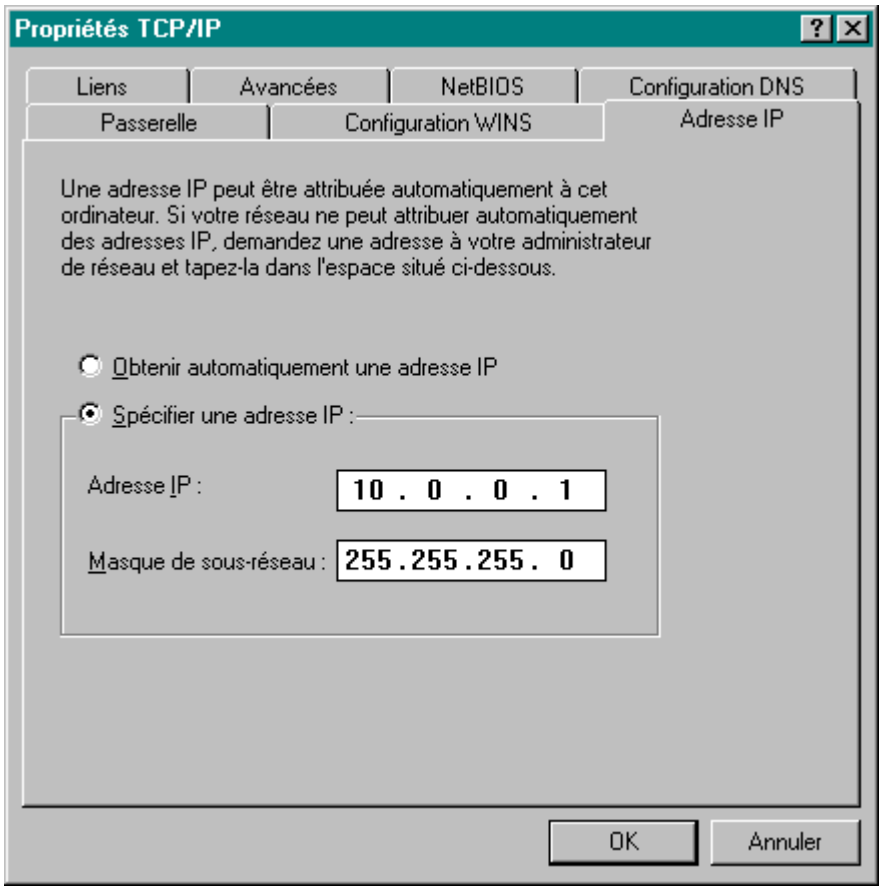
[125] = le Proxy = le Serveur

- Sélectionner *TCP/IP*
- Bouton *Propriétés*



- Sélectionner *Spécifier une adresse IP* :

[126] attention : pas sur la connexion à Internet



- Saisir ces valeurs[127]
- Bouton *OK*

Spécifier le port

- port : 6588[128]

Ouvrir ce port dans le poste principal comme dans les postes secondaires.

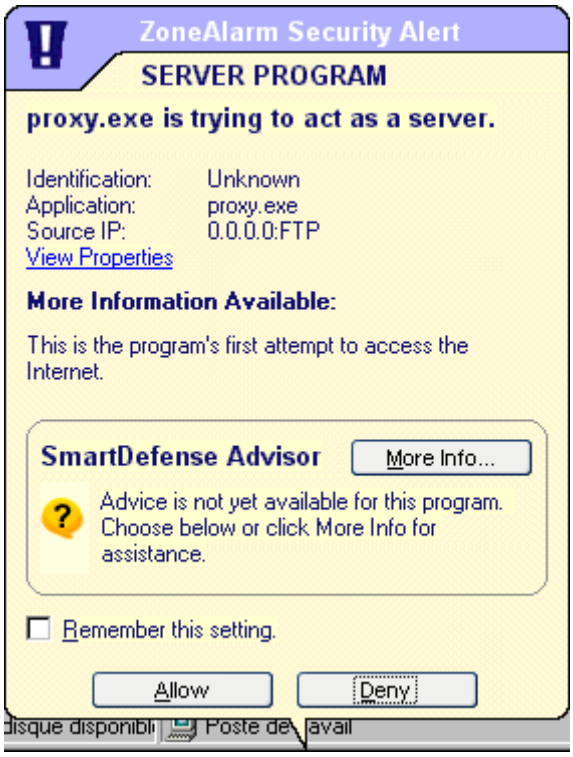
Installer le serveur proxy

Clic sur le fichier de distribution du logiciel + suivre les indications des panneaux.

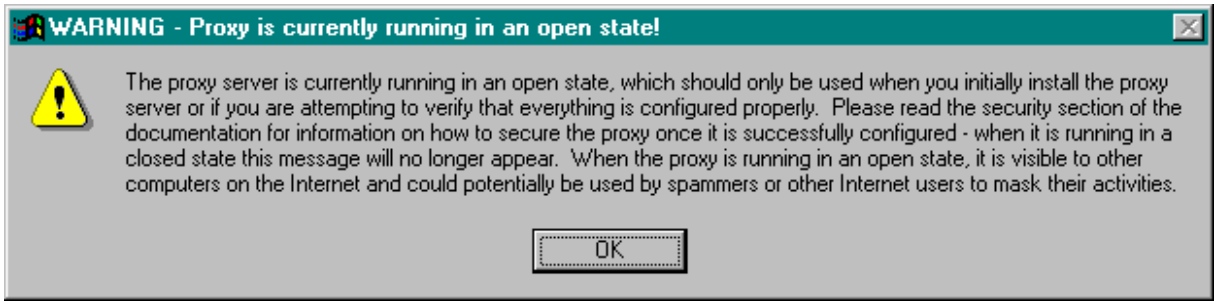
A la première utilisation

Le Firewall demande l'autorisation :

[127] Sur les autres machines, incrémenter de 1
[128] nécessaire pour utiliser Internet explorer



- accorder l'autorisation



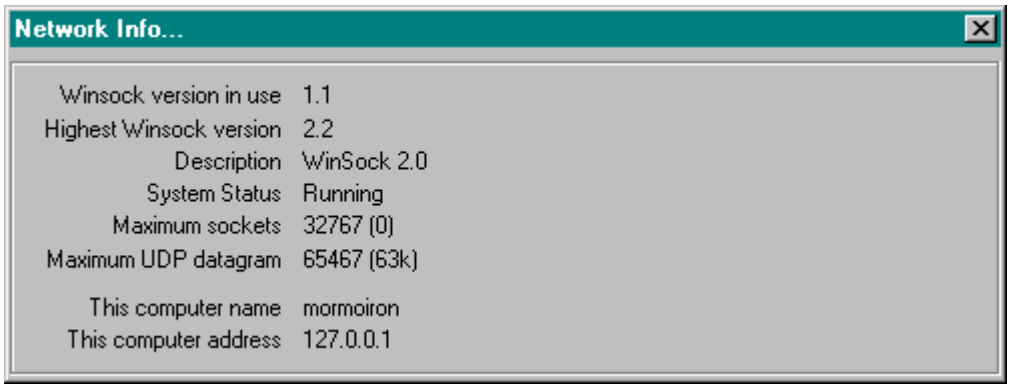
- au début, le Proxy est en mode *Ouvert*[129]

Configurations

L'icône AnalogX est apparue dans la zone de notification

- clic droit sur l'icône
- fonction *Net info*

[129] voir par ailleurs



Les postes secondaires

Sur chaque poste secondaire, il faut :

- *vérifier que TCP/IP est activé*
- *choisir une adresse IP*
- *configurer la connexion Internet*
- *configurer la messagerie*
- *configurer le client FTP*

Vérifier que TCP/IP est activé

Procéder comme pour le poste principal.

Choisir une adresse IP

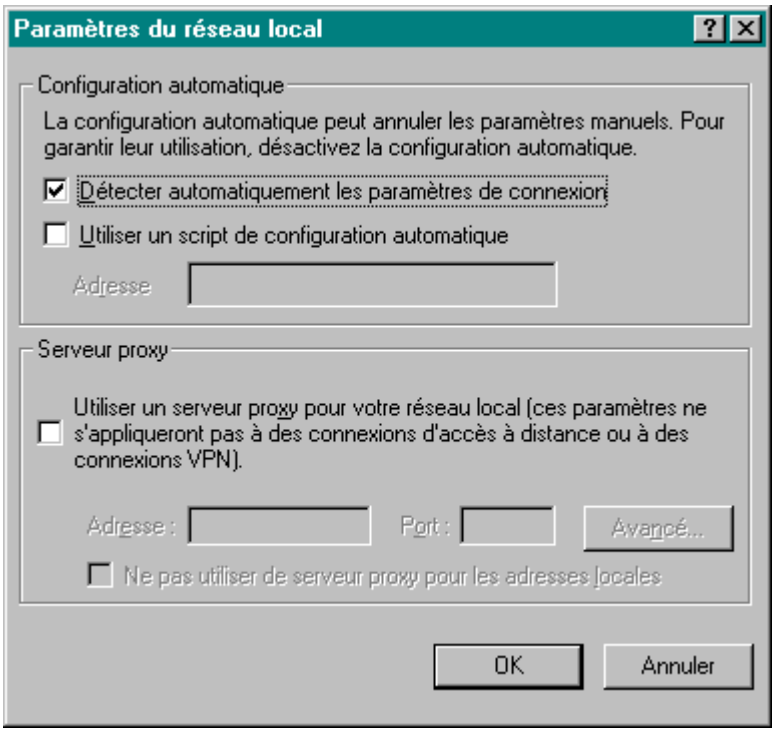
- adresse : 10.0.0.2 pour le premier, 10.0.0.3 pour le deuxième, …
- mask : 255.255.255.0

Procéder comme pour le poste principal.

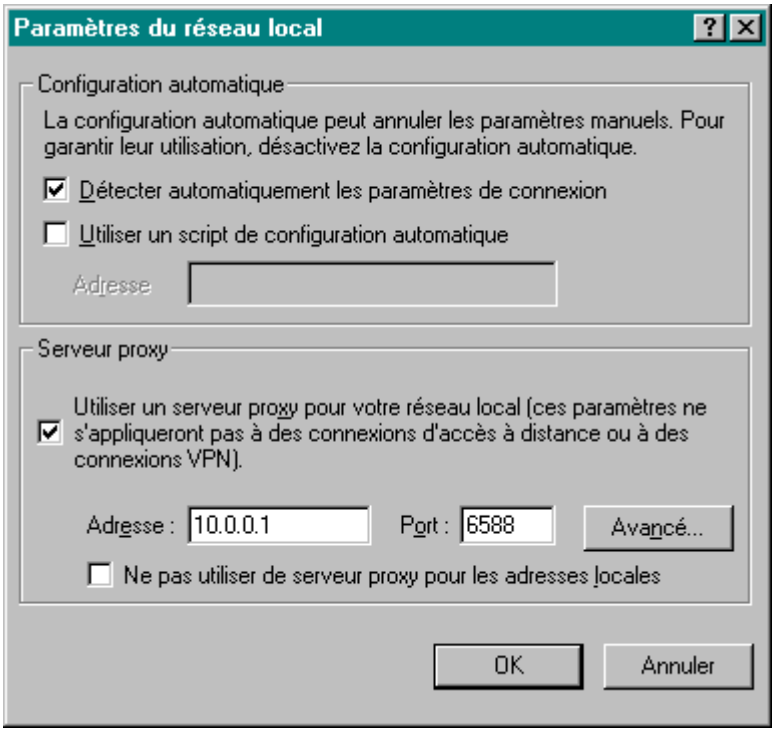
Configurer la connexion Internet

Dans Internet explorer :

- aller dans *Panneau de configuration/Options Internet*
- Onglet *Connexions*
- Bouton *Paramètres réseau*



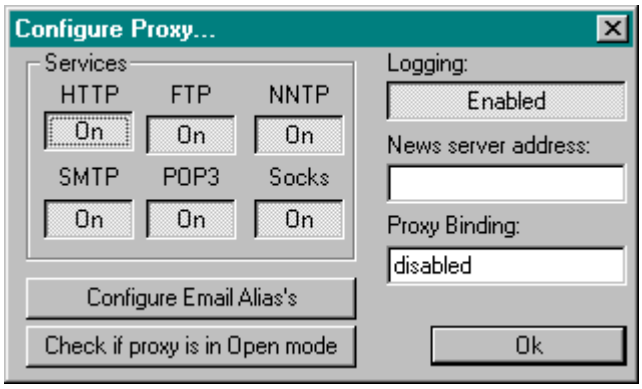
- Section *Serveur proxy*, sélectionner *Utiliser un serveur Proxy …*



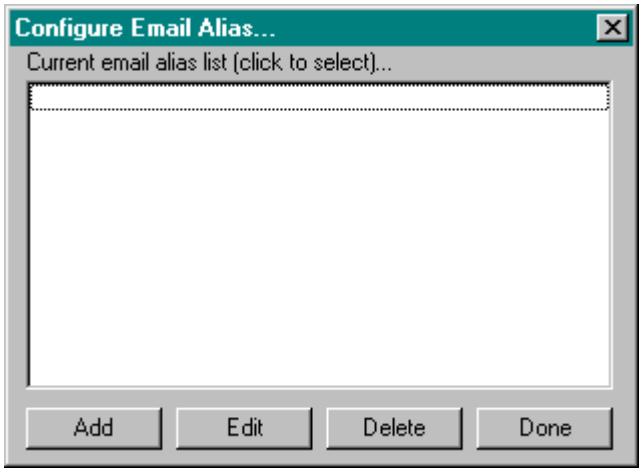
- Saisir les données comme ci dessus
- Bouton *OK*

Configurer la messagerie

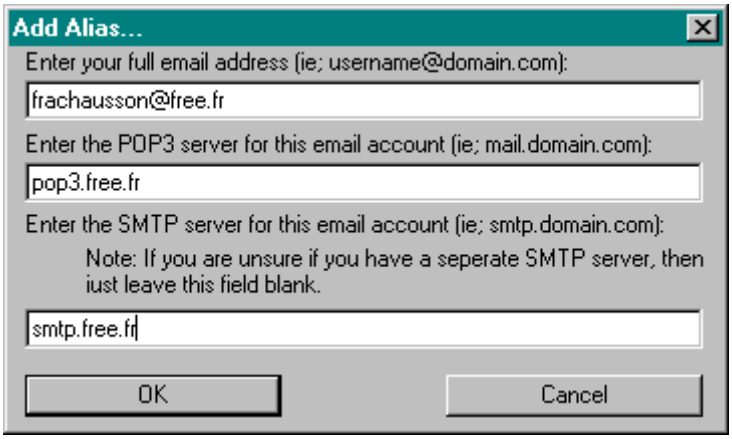
Ouvrir le menu *Configure*



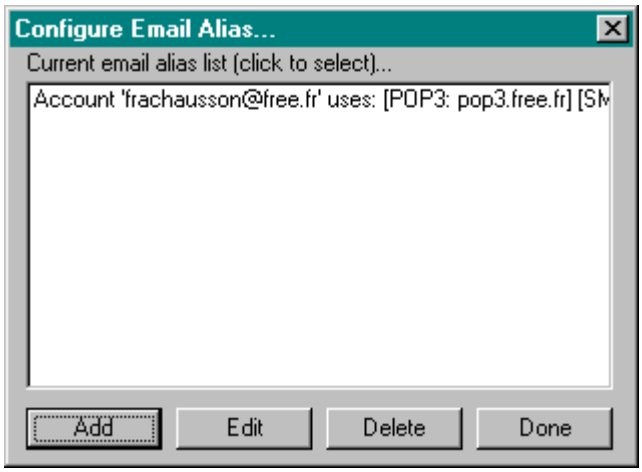
- Bouton *Configure Email alias's*



- Bouton *Add*



- Saisir les paramètres de messagerie



Parallèlement, dans le logiciel de messagerie[130] :

- Remplacer le paramétrage existant du user[131] par l'adresse IP du proxy : 10.0.0.1
- Procéder exactement de la même manière pour les paramétrages POP3 et SMTP

Configurer FTP

A compléter

Vérifications d'installation

Depuis le poste principal :

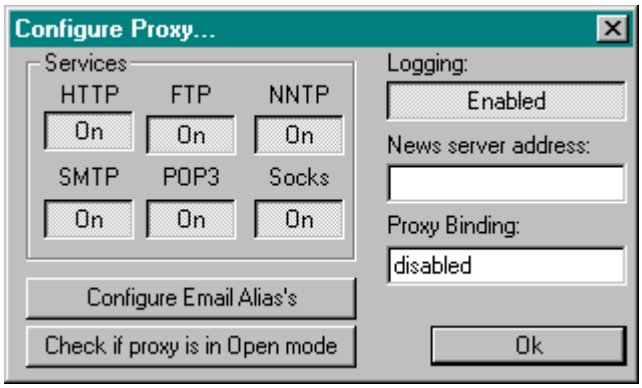
- Faire *Démarrer/Exécuter*
- Commande *cmd*
- Dans la fenêtre DOS, commande *ping*

A compléter

Post installation

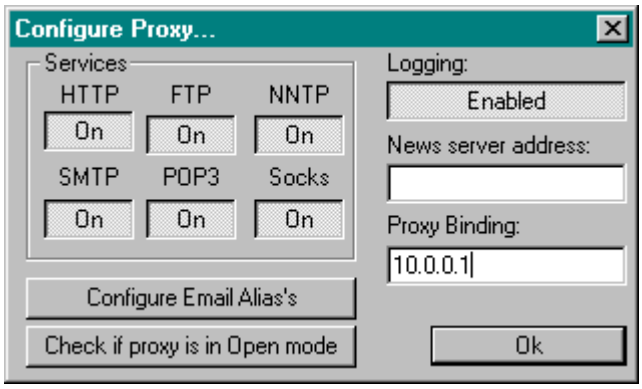
Dans le menu *Configure* :

- Par sécurité, « fermer » le Proxy



[130] Outlook express, Eudora, …
[131] dans cet exemple : frachausson@free.fr

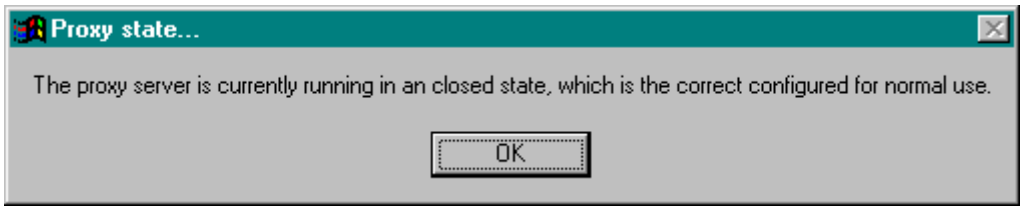
- Remplacer *disabled* par l'adresse IP du Proxy



Le Proxy n'échangera qu'avec des systèmes s'adressant à lui.

Vérification

- Menu *Configure*
- Bouton *Check if proxy is in open mode*



Installer un serveur WEB

Pour cela, il faut :

- Utiliser trois logiciels gratuits :
  - *Apache* (serveur Web)
  - *MySQL* (gestionnaire de bases de données)
  - *PHP* (interpréteur du langage du même nom)
- Disposer d'une adresse IP fixe ou utiliser un service de DNS dynamique
- Configurer le routeur et le pare-feu pour que le port 80 du serveur soit ouvert au Web

Voir http://www.01net.com/article/310299.html

Annexes

Paramétrer une connexion téléphonique

L'accès à Internet passe obligatoirement par une connexion physique[132] à un prestataire d'accès Internet[133].

La plupart des PAI proposent une offre gratuite de connexion par le réseau téléphonique commuté[134].

Pour l'utiliser, il n'est souvent[135] pas nécessaire de souscrire un abonnement au préalable.

Néanmoins, il faut avoir pu aller au préalable sur le site du PAI et créer un compte[136][137] car les informations de ce compte seront nécessaires dans l'installation décrite ci dessous.

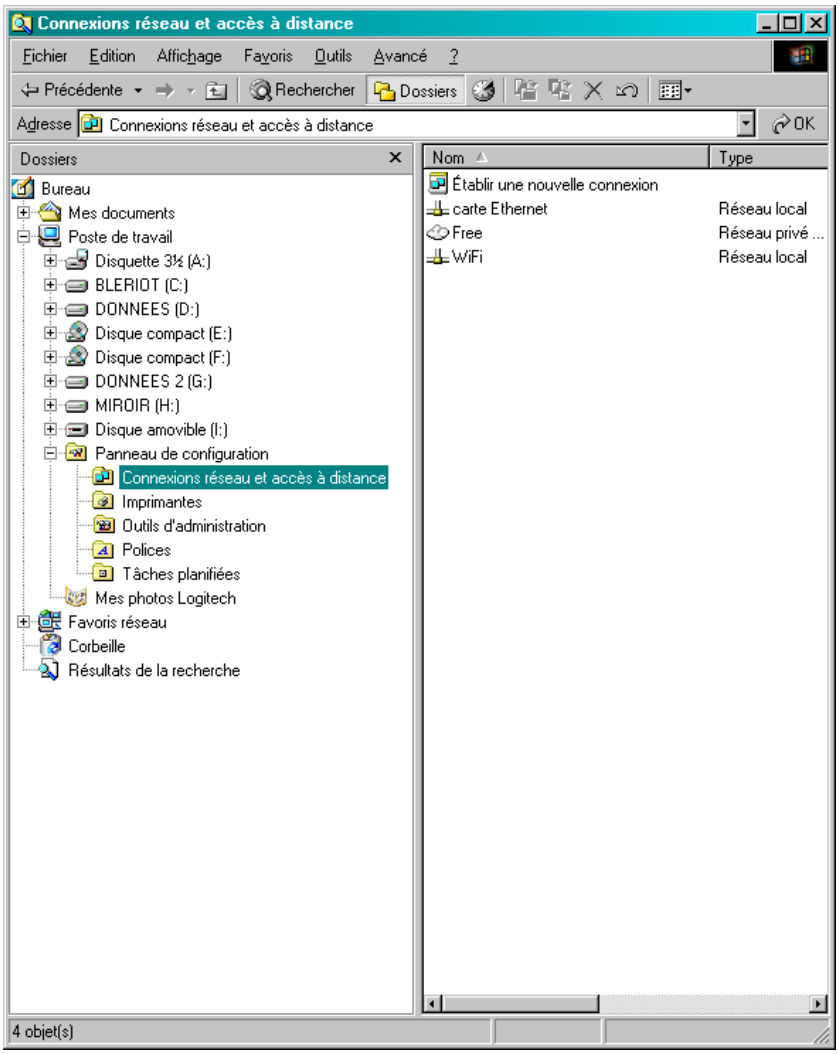
Installation

Pour créer dans Windows la description d'une connexion Internet par le réseau téléphonique commuté, procéder comme ça :

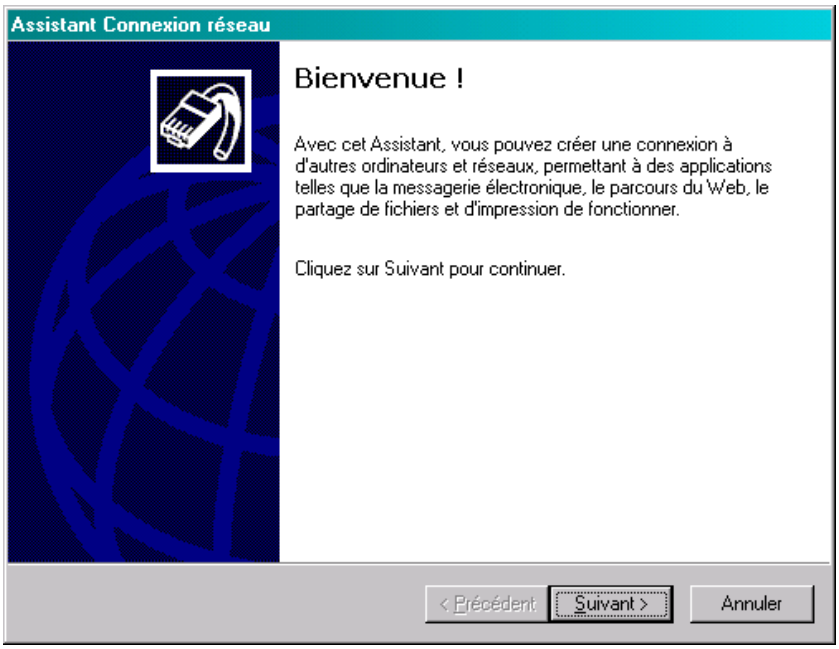
Dans l'Explorateur[138] :

- Sélectionner *Panneau de configuration/Connexion réseau …*

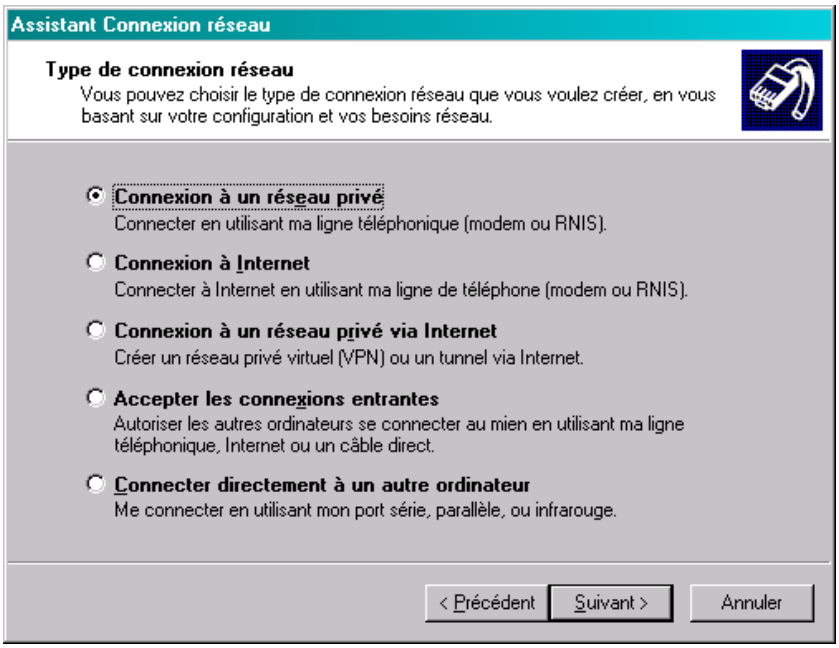
[132] téléphone, ADSL, câble, …
[133] = PAI
[134] = RTC
[135] ça dépend du PAI
[136] un compte = identifiant + mot de passe
[137] pour créer un compte chez Free, voir le document *Utiliser la messagerie Free*
[138] les exemples montrés ici sont extraits d'un poste en W2000, de présentation parfois un peu différente de celle d'un poste en WinXP



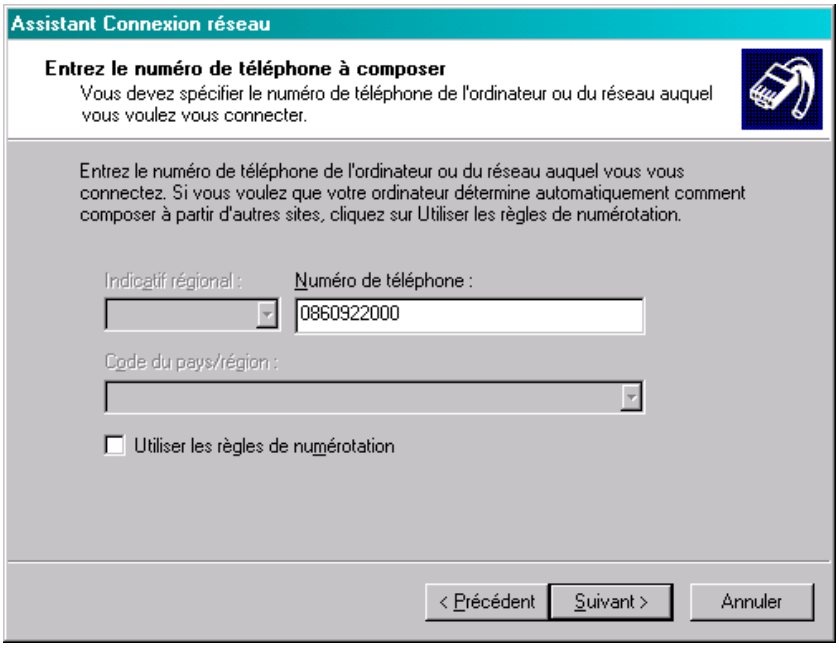
- 2 clics sur *Etablir une nouvelle …*



- bouton *Suivant*

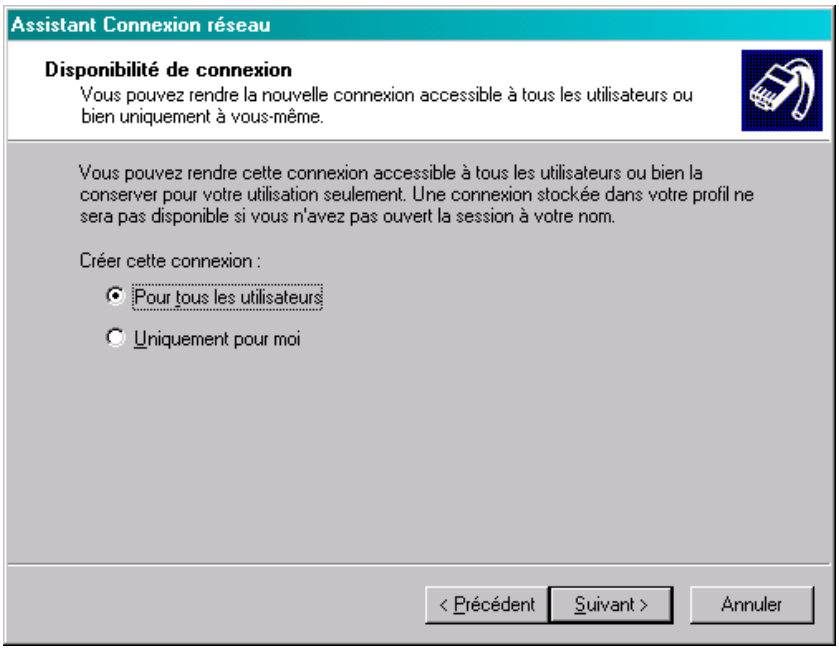


- bouton *Suivant*

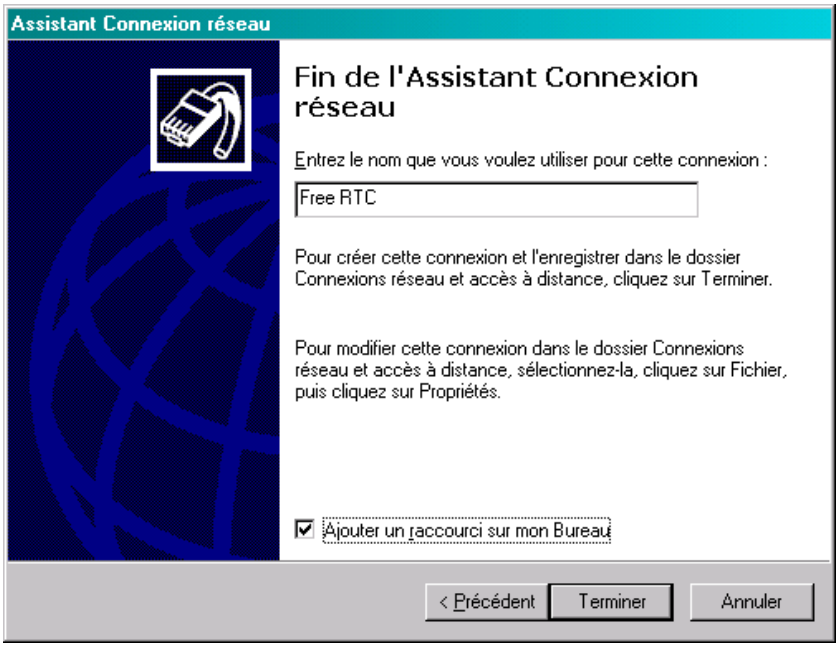


- saisir le numéro d'appel[139] du PAI + bouton *Suivant*

[139] ici : celui de Free



- bouton *Suivant*



- saisir le nom sous lequel cette connexion apparaîtra sur le Bureau[140]
- clic dans la case *Ajouter un raccourci …*
- bouton *Terminer*

La connexion se lance automatiquement une fois créée :

[140] et ailleurs

- saisir l'identifiant créé chez le PAI
- saisir le mot de passe créé chez le PAI
- clic sur la case *Enregistrer …*
- bouton *Composer*

Le poste va lancer la première connexion avec le PAI.

Utilisation courante

L'installation a créé une icône sur le Bureau :


Free RTC.lnk

Utilisation simple

Il est possible de lancer cette connexion en double cliquant sur cette icône ; en résultat, le poste sera connecté physiquement au PAI.

Il restera à lancer la messagerie, Internet Explorer, …

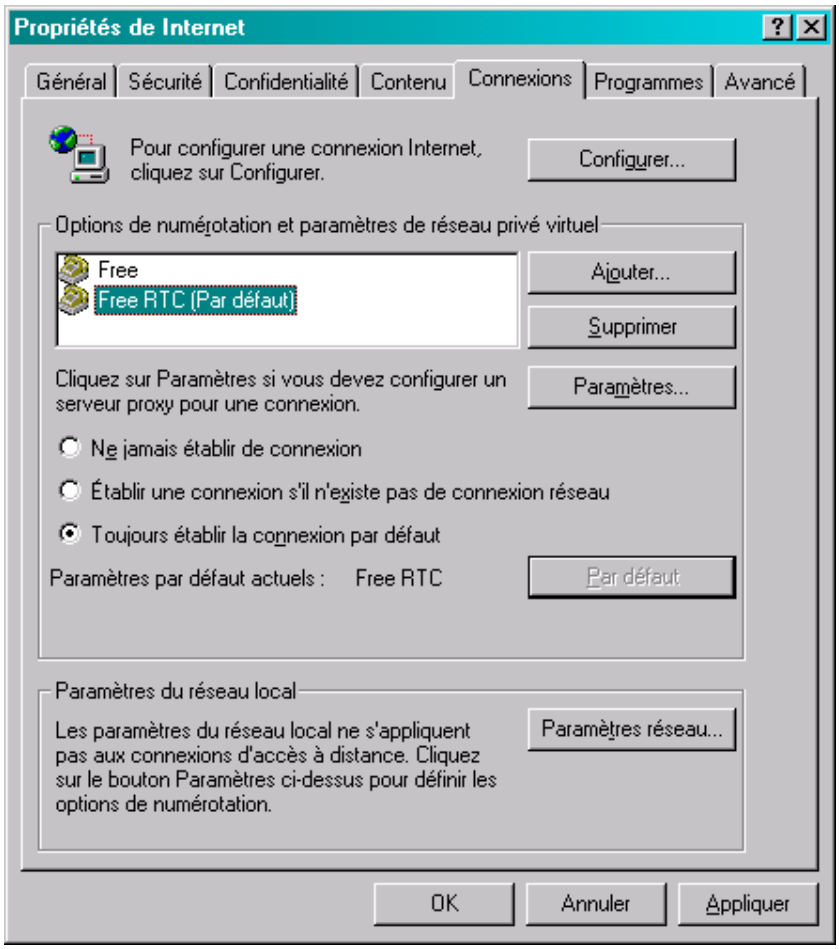
Utilisation intégrée

Pour utiliser cette connexion de manière intégrée à Internet Explorer, la messagerie, …, il faut faire des modifications dans les *options Internet*.

Pour ça :

- Aller dans *Panneau de configuration/Options Internet*

- Dans l'onglet *Connexions*
- Sélectionner la connexion créée, ici *Free RTC*
- Clic sur le bouton *Toujours établir …*
- Clic sur le bouton *Par défaut*



La connexion choisie apparaît maintenant *Par défaut*

- Bouton *OK*

Le lancement d'Internet Explorer[141], de la messagerie provoquera l'établissement de la connexion.

Deconnexion

Parmi plusieurs solutions :

- Sur le Bureau, clic droit sur l'icône de la connexion
- Sélectionner *Déconnecter*

Avertissement

La fermeture de Internet Explorer, de la messagerie n'interrompt pas automatiquement la connexion téléphonique[142].

Vérification

Pour s'assurer que la ligne a été raccrochée, il suffit de décrocher un téléphone et de vérifier la présence de la tonalité habituelle[143].

[141] aussi pour Outlook ?
[142] le compteur continue à tourner
[143] à défaut, recommencer la deconnexion

Références techniques

Internet Explorer v6

Il supporte :
- HTML 4.0
- CSS level 1 + une petite partie de CSS level 2
- DOM level 1
- MSXML 3.0
- …

Au besoin, consulter :
- IE v6 : http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnie60/html/cssenhancements.asp
- HTML 4.0.1 : http://www.w3schools.com/html/html_reference.asp
- CSS level 2 : http://www.w3schools.com/css/css_reference.asp

DNS

Pour Domain Name Server, cette fonction permet au réseau de transformer un nom de domaine[144] (www.monsite.com) en une adresse IP numérique[145] (157.45.12.67) et réciproquement.

Mettre en œuvre une connexion

Il faut établir le lien avec le DNS du PAI car il ne peut être accéder par son Hostname[146].

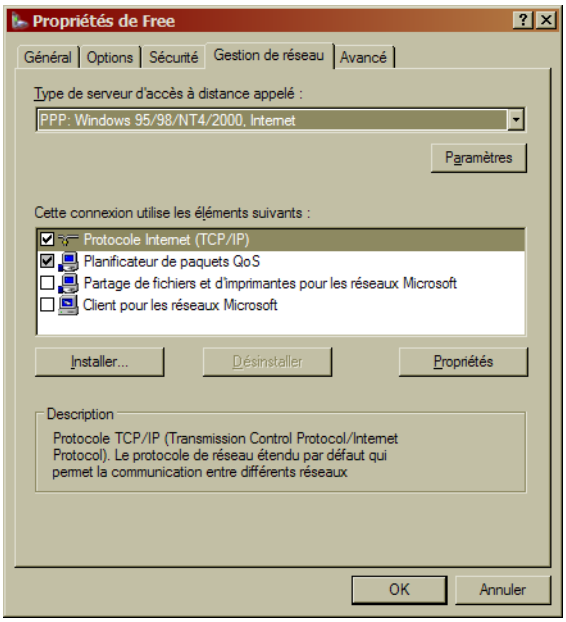
Pour ça, il faut spécifier l'adresse IP du DNS (les 2 DNS en général) dans les Propriétés de la connexion.

En général

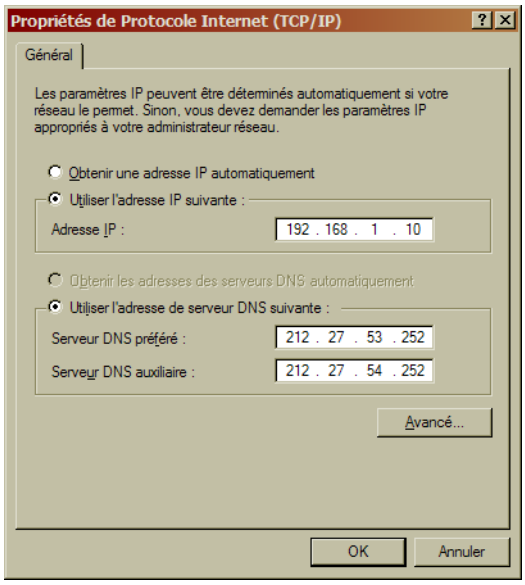
Pour commencer, noter d'abord l'adresse des DNS du PAI[147].

Dans l'Explorateur :
- *Panneau de configuration/ Connexions réseau*
- Clic droit sur la connexion concernée
- *Propriétés*
- Onglet *Gestion de réseau*

[144] une notion logique
[145] une notion physique
[146] eh Oui, c'est lui qui les traduit pour autant qu'il soit accédé
[147] information trouvée dans les documents transmis par le PAI, par Internet, …



- Sélectionner *TCP/IP*
- *Propriétés*



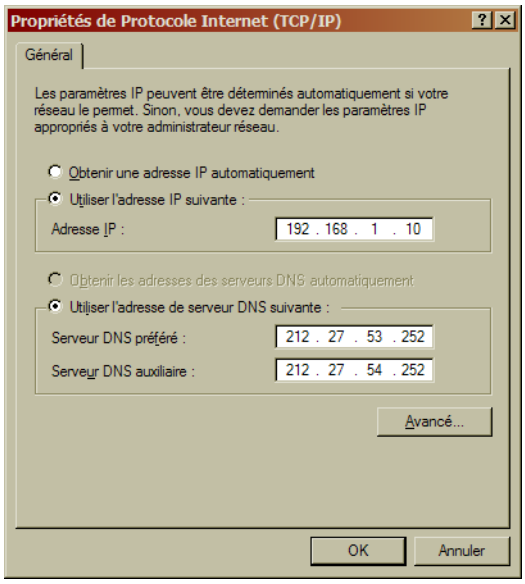
- Saisir :
  - Les adresses des 2 DNS notées précédemment
- Bouton *OK*
- Bouton *OK*

Connexion en adresse fixe

Pour une connexion en adresse fixe :

- Saisir :
  - l'adresse IP privée[148] fixe choisie dans le champ *Adresse IP*
  - le masque du sous-réseau (255.255.255.0)
  - Au besoin, la passerelle (192.168.1.1)

[148] cette adresse ne peut pas être une adresse publique car seul le PAI pourrait alors décider qu'elle soit fixe



Adresse dynamique ou adresse fixe ?

- Adresse dynamique : pour un réseau d'entreprise, complexe, avec de nombreux postes
- Adresse fixe : pour un réseau familial, avec quelques postes
- Adresse mixte : pour un réseau avec la majorité des postes en adresse dynamique et quelques postes en adresse fixe

Adressage mixte

Il faut isoler chaque groupe dans une plage d'adresse :

- Adresse dynamique : par exemple de 192.168.1.2 à 192.168.1.200
- Adresse fixe : par exemple de 192.168.1.200 à 192.168.1.254

La spécification est faite par un paramétrage dans le Routeur.

A défaut de cette précaution, le DHCP pourrait attribuer une adresse dynamique qui serait identique à une adresse fixe existante.

HijackThis, interprétation

En résumé

Détruire : **R3, F0, O1, O7, O13**

En détail

A l'URL : http://www.zebulon.fr/articles/HijackThis.php
HijackThis est un outil capable de traquer les hijackers présents sur votre PC. Ces modifications non sollicitées ont différents effets comme par exemple le détournement de la page d'accueil d'Internet Explorer, l'insertion d'un composant dans la barre du navigateur ou encore le détournement d'adresse IP via le fichier Hosts. Le programme liste les différents endroits où sont susceptibles de se cacher des hijackers et vous permet ainsi de supprimer les entrées suspectes. Malheureusement, l'interprétation de ces listes (ou logs) n'est pas chose aisée et bien souvent l'utilisateur ne sait si tel ou tel élément doit être supprimé. Ce tutoriel va nous permettre d'y voir plus clair.

Reproduit sur Zebulon avec la permission de Merijn, l'auteur du logiciel. Zebulon assure un support en ligne ici. Pous pouvez télécharger HijackThis ici.
Sur les forums de SpywareInfo, beaucoup d'internautes, étrangers au domaine du piratage de navigateur postent des discussions demandant de l'aide pour l'interprétation des listes d'HijackThis, parce qu'ils ne comprennent pas quels éléments sont bons et quels éléments sont nuisibles.
Ceci est un guide de base relatif à la signification des éléments de la liste, et quelques conseils pour les interpréter vous-mêmes. Ceci ne remplace en aucune manière l'aide à demander sur les forums qualifiés mais vous permet de comprendre un peu mieux la liste.
Vue d'ensemble
Chaque ligne d'un log d'HijackThis démarre avec un nom de section. (Pour plus d'informations techniques, cliquez sur 'Info' dans la fenêtre principale et descendre. Sélectionnez une ligne et cliquez sur 'More info on this item'.)
Sur le plan pratique, cliquez ci-dessous, sur le code de la section sur laquelle vous voulez de l'aide :
R0, R1, R2, R3 - URL des pages de Démarrage/Recherche d'Internet Explorer
F0, F1 - Programmes chargés automatiquement -fichiers .INI
N1, N2, N3, N4 - URL des pages de Démarrage/Recherche de Netscape/Mozilla
O1 - Redirections dans le fichier Hosts
O2 - Browser Helper Objects
O3 - Barres d'outils d'Internet Explorer
O4 - Programmes chargés automatiquement -Base de Registre et dossier Démarrage
O5 - Icônes d'options IE non visibles dans le Panneau de Configuration
O6 - Accès aux options IE restreints par l'Administrateur
O7 - Accès à Regedit restreints par l'Administrateur
O8 - Eléments additionnels du menu contextuel d'IE
O9 - Boutons additionnels de la barre d'outils principale d'IE ou éléments additionnels du menu 'Outils' d'IE
O10 - Pirates de Winsock
O11 - Groupes additionnels de la fenêtre 'Avancé' des Options d'IE
O12 - Plugins d'IE
O13 - Piratage des DefaultPrefix d'IE (préfixes par défaut)
O14 - Piratage de 'Reset Web Settings' (réinitialisation de la configuration Web)
O15 - Sites indésirables de la Zone de confiance
O16 - Objets ActiveX (alias Downloaded Program Files - Fichiers programmes téléchargés)
O17 - Pirates du domaine Lop.com
O18 - Pirates de protocole et de protocoles additionnels
O19 - Piratage de la feuille de style utilisateur

R0, R1, R2, R3 - Pages de démarrage et de recherche d'IE
Ce à quoi çà ressemble :
```
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page
= http://www.google.com/
R1 - HKLM\Software\Microsoft\Internet
Explorer\Main,Default_Page_URL = http://www.google.com/
R2 - (this type is not used by HijackThis yet)
R3 - Default URLSearchHook is missing
```
Que faire :
Si vous reconnaissez l'adresse à la fin de la ligne comme votre page de démarrage ou votre

moteur de recherche, c'est bon. sinon, cochez la et HijackThis la corrigera (bouton "Fix It"). Pour les éléments R3, corrigez les toujours sauf si çà concerne un programme que vous reconnaissez, comme Copernic.

F0, F1, F2, F3 - Programmes chargés automatiquement -fichiers .INI
Ce à quoi çà ressemble :
```
F0 - system.ini: Shell=Explorer.exe Openme.exe
F1 - win.ini: run=hpfsched
```
Que faire :
Les éléments F0 sont toujours nuisibles, donc corrigez les.
Les éléments F1 sont généralement de très vieux programmes qui sont sans problème, donc vous devriez obtenir plus d'informations à partir de leur nom de fichier pour voir s'ils sont bons ou nuisibles.
La "Startup List de Pacman"[149] peut vous aider à identifier un élément.

N1, N2, N3, N4 - Pages de démarrage et de recherche de Netscape/Mozilla
Ce à quoi çà ressemble :
```
N1 - Netscape 4: user_pref("browser.startup.homepage",
"www.google.com"); (C:\Program
Files\Netscape\Users\default\prefs.js)
N2 - Netscape 6: user_pref("browser.startup.homepage",
"http://www.google.com"); (C:\Documents and
Settings\User\Application
Data\Mozilla\Profiles\defaulto9t1tfl.slt\prefs.js)
N2 - Netscape 6: user_pref("browser.search.defaultengine",
"engine://C%3A%5CProgram%20Files%5CNetscape%206%5Csearchplugin
s%5CSBWeb_02.src"); (C:\Documents and
Settings\User\Application
Data\Mozilla\Profiles\defaulto9t1tfl.slt\prefs.js)
```
Que faire :
D'habitude les pages de démarrage et de recherche de Netscape et Mozilla sont bonnes. Elles sont rarement piratées ; seul Lop.com est connu pour ce faire. Si vous voyiez une adresse que vous ne reconnaitriez pas comme votre page de démarrage ou de recherche, faites la corriger par HijackThis.

O1 – Redirections dans le fichier Hosts
Ce à quoi çà ressemble :
```
O1 - Hosts: 216.177.73.139 auto.search.msn.com
O1 - Hosts: 216.177.73.139 search.netscape.com
O1 - Hosts: 216.177.73.139 ieautosearch
O1 - Hosts file is located at C:\Windows\Help\hosts
```
Que faire :
Ce piratage va rediriger l'adresse de droite vers l'adresse IP de gauche. Si l'IP ne correspond pas à l'adresse, vous serez redirigé vers un mauvais site chaque fois que vous entrerez cette adresse. Vous pouvez toujours les faire corriger par HijackThis, sauf si vous avez mis ces lignes à bon escient dans votre fichier Hosts.
Le dernier élément est quelquefois rencontré dans 2000/XP lors d'une infection Coolwebsearch. Corrigez toujours cet élément, ou faites le réparer automatiquement par CWShredder.

[149] URL : http://www.sysinfo.org/startuplist.php

O2 - Browser Helper Objects
Ce à quoi çà ressemble :
```
O2 - BHO: Yahoo! Companion BHO - {13F537F0-AF09-11d6-9029-0002B31F9E59} - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL
O2 - BHO: (no name) - {1A214F62-47A7-4CA3-9D00-95A3965A8B4A} - C:\PROGRAM FILES\POPUP ELIMINATOR\AUTODISPLAY401.DLL (file missing)
O2 - BHO: MediaLoads Enhanced - {85A702BA-EA8F-4B83-AA07-07A5186ACD7E} - C:\PROGRAM FILES\MEDIALOADS ENHANCED\ME1.DLL
```
Que faire :
Si vous ne reconnaissez pas directement un nom de Browser Helper Object, utilisez la "BHO & Toolbar List de TonyK" pour le trouver à partir de son identifieur de classe (CLSID, le nombre entre accolades) et déterminer s'il est bon ou nuisible. Dans la BHO List, 'X' signifie spyware et 'L' signifie bon.

O3 - Barres d'outils d'IE
Ce à quoi çà ressemble :
```
O3 - Toolbar: &Yahoo! Companion - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL
O3 - Toolbar: Popup Eliminator - {86BCA93E-457B-4054-AFB0-E428DA1563E1} - C:\PROGRAM FILES\POPUP ELIMINATOR\PETOOLBAR401.DLL (file missing)
O3 - Toolbar: rzillcgthjx - {5996aaf3-5c08-44a9-ac12-1843fd03df0a} - C:\WINDOWS\APPLICATION DATA\CKSTPRLLNQUL.DLL
```
Que faire :
Si vous ne reconnaissez pas directement un nom de Browser Helper Object's, utilisez la "BHO & Toolbar List de TonyK" pour le trouver à partir de son identifieur de classe (CLSID, le nombre entre accolades) et déterminer s'il est bon ou nuisible. Dans la Toolbar List, 'X' signifie spyware et 'L' signifie bon.
Si elle n'est pas dans la liste et que le nom ressemble à une chaine de caractères aléatoires, et que le fichier est dans le dossier 'Application Data' (comme le dernier exemple ci-dessus), c'est probablement Lop.com, et vous devez à coup sûr le faire réparer par HijackThis.

O4 - Programmes chargés automatiquement -Base de Registre et dossier Démarrage
Ce à quoi çà ressemble :
```
O4 - HKLM\..\Run: [ScanRegistry] C:\WINDOWS\scanregw.exe /autorun
O4 - HKLM\..\Run: [SystemTray] SysTray.Exe
O4 - HKLM\..\Run: [ccApp] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
O4 - Startup: Microsoft Office.lnk = C:\Program Files\Microsoft Office\Office\OSA9.EXE
O4 - Global Startup: winlogon.exe
```
Que faire :
Utilisez la Startup List de Pacman pour y trouver l'élément et déterminer s'il est bon ou nuisible.
Si l'élément indique un programme situé dans le groupe Démarrage (comme le dernier élément ci-dessus), HijackThis ne pourra pas le corriger si ce programme est encore en

mémoire. Utilisez le Gestionnaire des tâches de Windows (TASKMGR.EXE) pour stopper le processus avant de corriger.

O5 - Options IE non visibles dans le Panneau de configuration
Ce à quoi çà ressemble :
```
O5 - control.ini: inetcpl.cpl=no
```
Que faire :
Sauf si vous ou votre administrateur système avez caché l'icône à bon escient dans le Panneau de configuration, faites réparer par HijackThis.

O6 - Accès aux options IE restreints par l'Administrateur
Ce à quoi çà ressemble :
```
O6 - HKCU\Software\Policies\Microsoft\Internet
Explorer\Restrictions present
```
Que faire :
Sauf si vous avez activé l'option "Lock homepage from changes" (verrouiller le changement de page de démarrage) dans Spybot S&D, ou si votre administrateur système l'a mise en place, faites réparer par HijackThis.

O7 - Accès à Regedit restreints par l'Administrateur
Ce à quoi çà ressemble :
```
O7 -
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
, DisableRegedit=1
```
Que faire :
Toujours faire réparer par HijackThis, à moins que vous administrateur système ait mis cette restriction en place.

O8 - Eléments additionnels du menu contextuel d'IE (clic droit)
Ce à quoi çà ressemble :
```
O8 - Extra context menu item: &Google Search -
res://C:\WINDOWS\DOWNLOADED PROGRAM
FILES\GOOGLETOOLBAR_EN_1.1.68-DELEON.DLL/cmsearch.html
O8 - Extra context menu item: Yahoo! Search -
file:///C:\Program Files\Yahoo!\Common/ycsrch.htm
O8 - Extra context menu item: Zoom &In -
C:\WINDOWS\WEB\zoomin.htm
O8 - Extra context menu item: Zoom O&ut -
C:\WINDOWS\WEB\zoomout.htm
```
Que faire :
Si vous ne reconnaissez pas le nom de l'élément dans le menu contextuel d'IE (clic droit), faites réparer par HijackThis.

O9 - Boutons additionnels de la barre d'outils principale d'IE ou éléments additionnels du menu 'Outils' d'IE
Ce à quoi çà ressemble :
```
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Messenger (HKLM)
O9 - Extra button: AIM (HKLM)
```

Que faire :
Si vous ne reconnaissez pas le nom du bouton ou de l'option du menu, faites réparer par HijackThis.

O10 - Pirates de Winsock
Ce à quoi çà ressemble :
```
O10 - Hijacked Internet access by New.Net
O10 - Broken Internet access because of LSP provider
'c:\progra~1\common~2\toolbar\cnmib.dll' missing
O10 - Unknown file in Winsock LSP: c:\program files\newton
knows\vmain.dll
```
Que faire :
Mieux vaut les réparer en utilisant LSPFix de Cexx.org, ou Spybot S&D de Kolla.de.
Notez que les fichiers 'unknown' (inconnus) dans la pile LSP ne seront pas corrigés par HijackThis, par sécurité.

O11 - Groupes additionnels de la fenêtre 'Avancé' des Options d'IE
Ce à quoi çà ressemble :
```
O11 - Options group: [CommonName] CommonName
```
Que faire :
Le seul pirate qui ajoute, jusqu'à maintenant, son propre groupe d'options à la fenêtre "Avancé" des options d'IE, est CommonName. Donc faites toujours corriger par HijackThis.

O12 - Plugins d'IE
Ce à quoi çà ressemble :
```
O12 - Plugin for .spop: C:\Program Files\Internet
Explorer\Plugins\NPDocBox.dll
O12 - Plugin for .PDF: C:\Program Files\Internet
Explorer\PLUGINS\nppdf32.dll
```
Que faire :
La plupart du temps, ils sont sains. Seul OnFlow ajoute un plugin dont vous ne voulez pas ici (.ofb).

O13 - Piratage des DefaultPrefix d'IE (préfixes par défaut)
Ce à quoi çà ressemble :
```
O13 - DefaultPrefix: http://www.pixpox.com/cgi-
bin/click.pl?url=
O13 - WWW Prefix: http://prolivation.com/cgi-bin/r.cgi?
O13 - WWW. Prefix: http://ehttp.cc/]http://ehttp.cc/?
```
Que faire :
Ceux-là sont toujours nuisibles. Faites réparer par HijackThis.

O14 - Piratage de "Reset Web Settings" (réinitialisation de la configuration Web)
Ce à quoi çà ressemble :
```
O14 - IERESET.INF: START_PAGE_URL=http://www.searchalot.com
```
Que faire :
Si l'URL n'est pas celle de votre Fournisseur d'Accès à Internet, faites réparer par HijackThis.

O15 - Sites indésirables de la Zone de confiance
Ce à quoi çà ressemble :
```
O15 - Trusted Zone: http://free.aol.com]http://free.aol.com
O15 - Trusted Zone: *.coolwebsearch.com
O15 - Trusted Zone: *.msn.com
```
Que faire :
La plupart du temps, seuls AOL et Coolwebsearch ajoutent en douce, des sites à la Zone de confiance. Si vous n'avez pas vous-même ajouté le domaine affiché, dans la Zone de confiance, faites réparer par HijackThis.

O16 - Objets ActiveX (alias Downloaded Program Files - Fichiers programmes téléchargés)
Ce à quoi çà ressemble :
```
O16 - DPF: Yahoo! Chat - h
ttp://us.chat1.yimg.com/us.yimg.com/i/chat/applet/c381/chat.ca
b
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave
Flash Object) - h
ttp://download.macromedia.com/pub/shockwave/cabs/flash/swflash
.cab
```
Que faire :
Si vous ne reconnaissez pas le nom de l'objet ou l'adresse à partir de laquelle il a été téléchargé, faites réparer par HijackThis. Si le nom ou l'URL contient des mots comme 'dialer', 'casino', 'free_plugin' etc., à coup sûr réparez.
SpywareBlaster de Javacool a une immense base de données des objets ActiveX malicieux qui peuvent être utilisés pour vérifier les CLSID. (cliquez droit dans la liste pour utiliser la fonction de recherche.)

O17 - Piratage du domaine Lop.com
Ce à quoi çà ressemble :
```
O17 - HKLM\System\CCS\Services\VxD\MSTCP: Domain = aoldsl.net
O17 - HKLM\System\CCS\Services\Tcpip\Parameters: Domain =
W21944.find-quick.com
O17 - HKLM\Software\..\Telephony: DomainName = W21944.find-
quick.com
O17 - HKLM\System\CCS\Services\Tcpip\..\{D196AB38-4D1F-45C1-
9108-46D367F19F7E}: Domain = W21944.find-quick.com
O17 - HKLM\System\CS1\Services\Tcpip\Parameters: SearchList =
gla.ac.uk
O17 - HKLM\System\CS1\Services\VxD\MSTCP: NameServer =
69.57.146.14,69.57.147.175
```
Que faire :
Si le domaine n'est pas celui de votre FAI ou du réseau de votre entreprise, faites réparer par HijackThis. Même chose pour les 'SearchList'.
Pour le 'NameServer' (serveur DNS), demandez à Google pour la ou les IP et çà sera facile de voir si c'est bon ou nuisible.

O18 - Pirates de protocole et de protocoles additionnels
Ce à quoi çà ressemble :
```
O18 - Protocol: relatedlinks - {5AB65DD4-01FB-44D5-9537-
3767AB80F790} - C:\PROGRA~1\COMMON~1\MSIETS\msielink.dll
O18 - Protocol: mctp - {d7b95390-b1c5-11d0-b111-0080c712fe82}
```

`O18 - **Protocol hijack: http** - {66993893-61B8-47DC-B10D-21E0C86DD9C8}`
Que faire :
Seuls quelques pirates la ramène ici. Les néfates connus sont 'cn' (CommonName), 'ayb' (Lop.com) et 'relatedlinks' (Huntbar), vous devez les faire réparer par HijackThis.
D'autres choses qu'on y voit sont non confirmés comme sains ou piratés par des spywares (par exemple le CLSID qui a été modifié). Dans ce dernier cas, faites réparer par HijackThis.

O19 - Piratage de la feuille de style utilisateur
Ce à quoi çà ressemble :
`O19 - User style sheet: c:\WINDOWS\Java\**my.css**`
Que faire :
Dans le cas d'un ralentissement du navigateur et de popups fréquents, faites réparer cet élément par HijackThis s'il apparaît dans la liste. Cependant, à partir du moment où seulement Coolwebsearch (http://www.spywareinfo.com/~merijn/cwschronicles.html) fait ceci, il est mieux d'utiliser CWShredder pour le corriger.

Notes importantes
Avant d'utiliser HijackThis, il est fortement conseillé d'effectuer les manipulations suivantes :
- supprimez tous vos fichiers Internet temporaires
- scannez vos disques avec un antivirus installé sur votre PC
- scannez vos disques avec un antivirus en ligne (voir ici)
- scannez votre machine avec Spybot - Search & Destroy
- utilisez CWShredder
Une fois ces actions effectuées, vous devriez avoir un système plus propre, je vous invite à lire quelques tutoriaux concernant les divers services et processus qui tournent sur votre machine et qui sont en rapport avec le log de HijackThis :
- le gestionnaire des tâches
- Msconfig
- les services

Voila, maintenant, vous êtes en mesure d'identifier une partie des services et processus qui tournent sur votre machine. Vous pouvez donc utiliser pleinement HijackThis. Si certaines lignes vous paraissent suspectes, vous pouvez les poster sur le forum, il est impératif de nous indiquer votre système d'exploitation, la nature du nettoyage (virus, bug, page de démarrage internet changée, optimisation du système, etc.), tout cela afin de répondre au mieux à vos attentes.

Pour l'utilisation du logiciel, cliquez sur le bouton *Scan* : la vérification des clés commence.

Si vous souhaitez nous faire parvenir le log de hijackthis, cliquez sur le bouton *Save Log* et enregistrez le dans votre répertoire courant. Ouvrez ensuite le fichier de log, sélectionnez tout et faites un copier/coller sur le post du forum. Après étude du log hijackthis, il vous suffira alors de cocher les lignes néfastes.

Une fois toutes les lignes néfastes cochées, cliquez sur le bouton *fix checked*, ce qui a pour effet de supprimer les lignes tout en créant un fichier backup pour chaque ligne dans le répertoire spécifique.

TCP/IP

TCP/IP est le protocole d'échange utilisé sur Internet.

Un des éléments de base est l'identification :

- Le serveur distant : par son adresse réseau, dite *adresse IP*[150]
- Le traitement recherché sur ce serveur : par le *port*

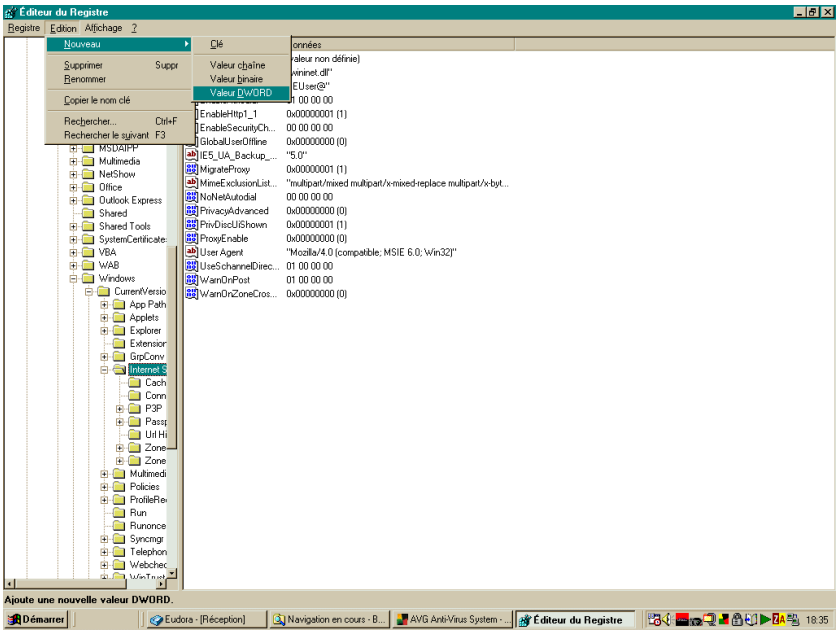
Certains ports ont une utilisation standard :

- FTP : 21
- Telnet : 23
- …

De manière générale, les ports 1-255 sont réservés à des utilisations standards.

Internet Explorer, télécharger plus de deux fichiers simultanément

- Faire *Démarrer/Exécuter/regedit*
- Aller dans *HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/InternetSettings*



- Créer deux nouvelles valeurs DWORD :
  - "MaxConnectionsPer1_0Server"=Dword:0000000a
  - "MaxConnectionsPerServer"=Dword: 0000000a
  -
- Avec :
  - Cocher case *Hexadecimale*
  - Saisir *64*

[150] exemple d'une adresse IP : 129.126.45.154

Alternative :

- 2 clics sur *10_ie_dl.zip*

Google toolbar

Installable depuis : http://toolbar.google.com/install

Les processus actifs du système

C'est à dire ceux qui se trouvent là de manière légitime[151] :

Csrss.exe : Sans ce service, toutes applications non 32 bits ne peut fonctionner, ce sous-système essentiel qui doit fonctionner en permanence.
DragDiag: Nom du processus lié à l'icône témoin de l'état de la connexion ADSL dans le cas d'un Modem Alcatel
RunDLL32.exe:C'est un exécutable utilisé par de Windows, il permet de charger toute sorte de fonctionnalité contenue dans des DLL. Pour information, l'icône du pilote Bewan USB apparaît sous ce nom dans les processus.
Explorer : C'est LE résident Windows, il permet d'afficher la structure de toutes les fenêtres, de la barre de tâche, du menu démarrer, etc..... Il ne doit pas être confondu avec l'explorateur Windows qui utilise le même fichier de programme !
Lsass.exe : Il s'agit du serveur local d'authentification de sécurité, il génère le processus responsable de l'authentification des utilisateurs par le service Winlogon.
PackethSvc.exe : Processus Réseau installé avec l'adapteur (Wan Network Driver) d'AOL 6.0, visible dans le Panneau de configuration / Outils d'administration / Service / " Virtual NIC Service ". Il apparaît dans les processus Windows même si AOL 6.0 n'est pas lancé. Ce même nom apparaît dans l'onglet " Service " de MsConfig. Au lancement d'AOL 6.0 ce processus se réactivera si l'on avait tenté de le désactiver.
Processus inactif du système : Correspond aux ressources processeur libres, le pourcentage est visible dans la colonne " CPU ". Quand le "processus inactif" est à 88 % par exemple ce la signifie que le CPU est utilisé à 12 % par les autres processus.
Services.exe : Il s'agit du " Service Control Manager " gestionnaire de contrôle des services, qui est responsable du démarrage, de l'arrêt et de l'interaction avec les services système.
Smss.exe : Il s'agit du sous-système de gestion de session (session manager subsystem), permet le démarrage de la session utilisateur.
Spoolsv.exe : Le service spooler est responsable de la gestion des travaux d'impression et de fax.

[151] ce qui ne veut pas dire que les autres sont illégitimes

Svchost.exe (peux apparaître plusieurs fois) : Processus qui agit en tant que serveur pour d'autres processus fonctionnant depuis des DLLs.
System : La plupart des thread (amorçages) du mode noyau fonctionnent en tant que processus System.
Taskmgr.exe : C'est le processus pour le gestionnaire des tâches lui-même ;-)
Winlogon.exe : Il s'agit du processus responsable de l'ouverture et la fermeture des différentes sessions Windows.

Contrôles d'usage professionnels

De nombreux employeurs ont maintenant mis sur pied et publié une charte d'utilisation du poste de travail par l'employé.

Le plus souvent, il est convenu que l'employé peut faire un usage personnel de son poste de travail pourvu que cet usage soit limité, à l'instar du téléphone.

Dans ces chartes, il est souvent convenu que :
- L'usage de la messagerie n'est pas limité
- L'accès aux sites Web est limité

Il est parfois précisé que l'employeur peut accéder aux contenus d'un échange, un mail par exemple, mais dans des conditions de publicité précises, à l'instar du téléphone ou du courrier postal.

A l'inverse, il arrive aussi que rien ne soit précisé, ce qui doit normalement correspondre à un hermétisme total des contenus vis à vis de l'employeur.

Accès messagerie

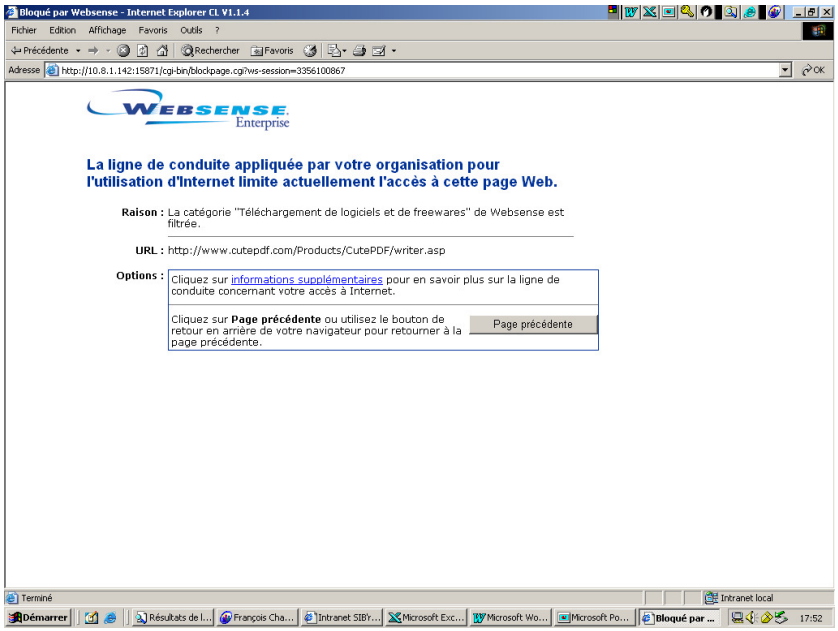
L'accès messagerie a parfois des limites :
- L'accès Internet n'est pas toujours attribué par défaut, limitant alors son usage à des échanges de mail internes à l'entreprise
- Il arrive parfois que tout message portant une pièce attachée cryptée[152] soit rejeté
- …

Accès Web

L'accès aux sites Web est souvent limité, soit dans le temps, restreint parfois à la pose de midi, soit dans l'espace Internet, en ne laissant l'accès qu'à certains sites sans qu'il soit possible d'en prédire le périmètre exact[153].

Un exemple de réponse à un accès à un site Web rejeté par le système de contrôle de l'employeur :

[152] Que l'anti virus ne peut pas ouvrir et tester
[153] des filtres basés sur des listes noires, blanches, … ?



Il s'agissait, dans cet exemple, d'accéder à un site Web proposant un téléchargement ; par ailleurs, les téléchargement de fichiers de format exécutables[154] sont fréquemment interdits.

A l'inverse, l'accès à des sites très publics, comme Google, Yahoo, Météo France, les Pages jaunes, la SNCF, la RATP, … est souvent possible.

HotSpots WiFi gratuit

Visiter :

- http://www.laptopkfe.com
- http://www.hot-spot.org
- http://dly.free.fr/site/article.php3
- …

Les options Internet

Dans Internet Explorer[155]

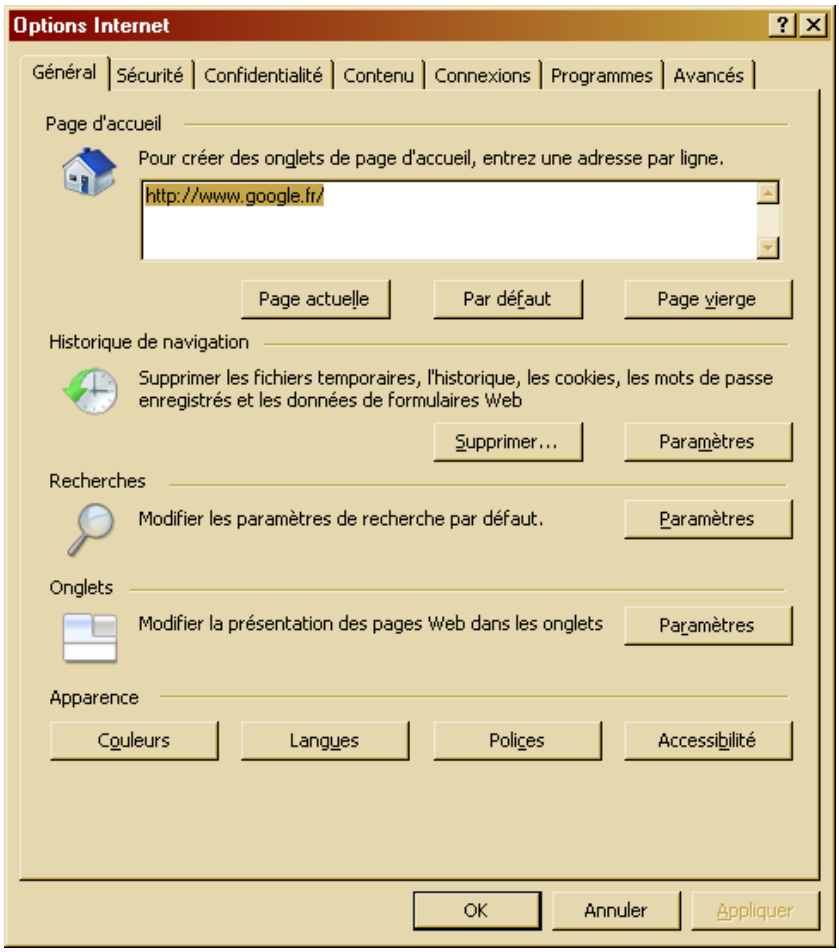
- Clic sur l'action *Outils*[156]
- Sélectionner *Options Internet*

Le panneau présenté propose plusieurs onglets différents.

Onglet Général

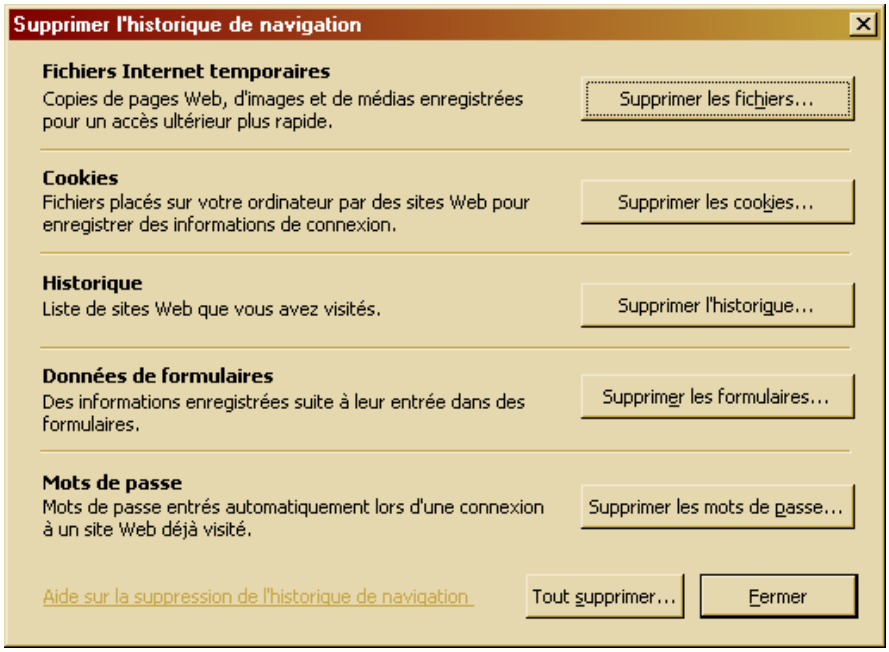
Faire un premier ménage :

[154] les extensions .EXE, …
[155] ou ailleurs
[156] A droite en haut

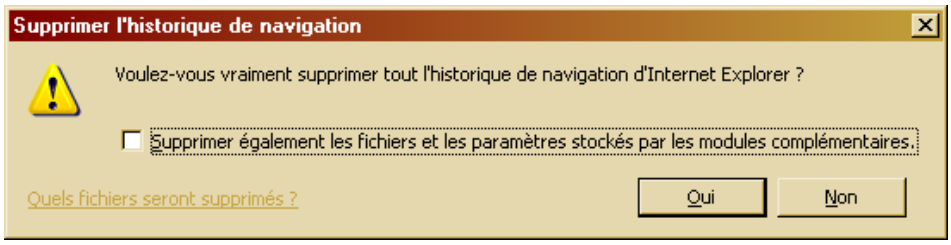


Dans la section *Historique de navigation* :

- Bouton *Supprimer*



- Bouton *Tout supprimer*



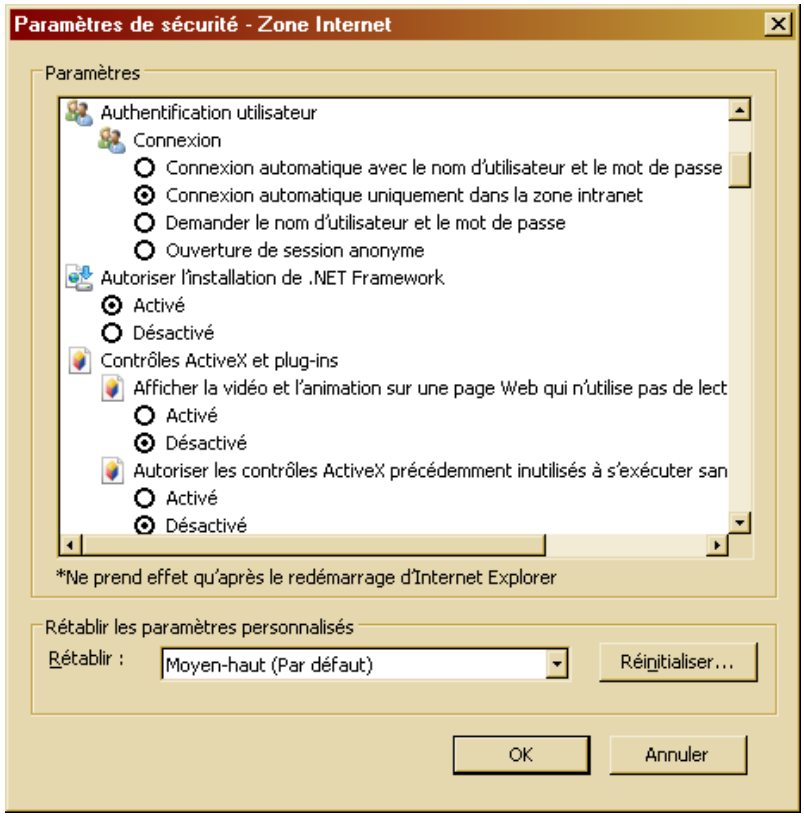
- Bouton *Oui*

Remarques :

- La suppression s'exerce sans délai mais son action n'est pas permanente[157]

Onglet Sécurité

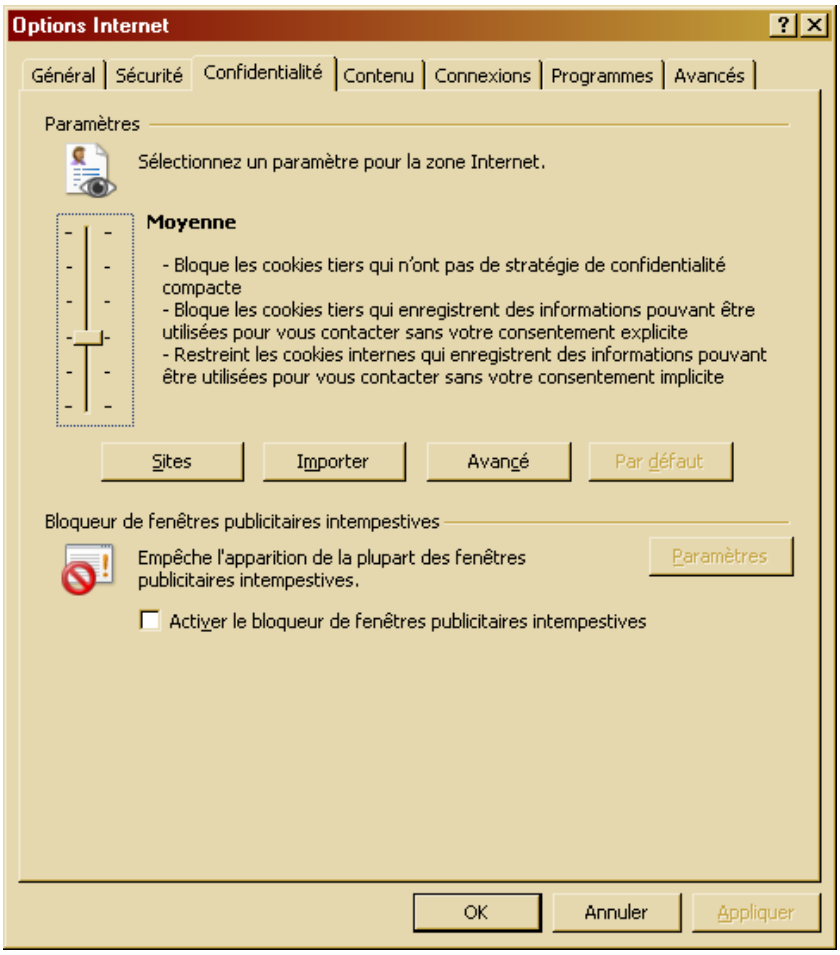
- Sélectionner *Internet*
- Bouton *Personnaliser le niveau*



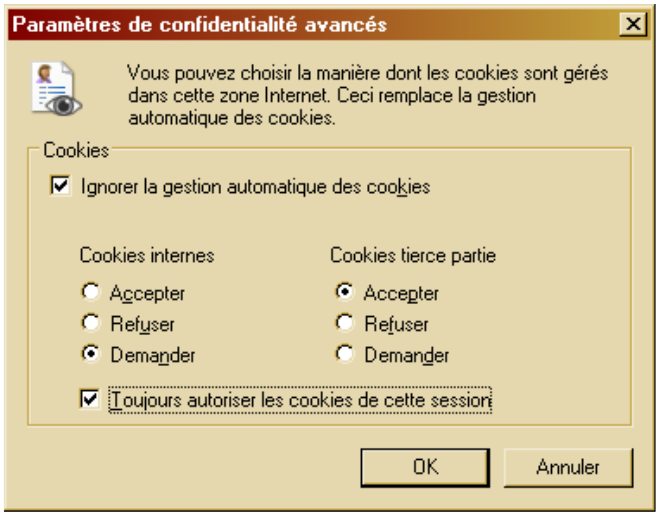
- Dans le domaine *Authentification utilisateur*
- Dans la section *Connexion,* cocher la case *Demander le nom d'utilisateur …*

Onglet Confidentialité

[157] Dit autrement, pour éviter plus tard l'accumulation des cookies, …, il faudra exercer de nouveau cette action



- Bouton *Avancé*

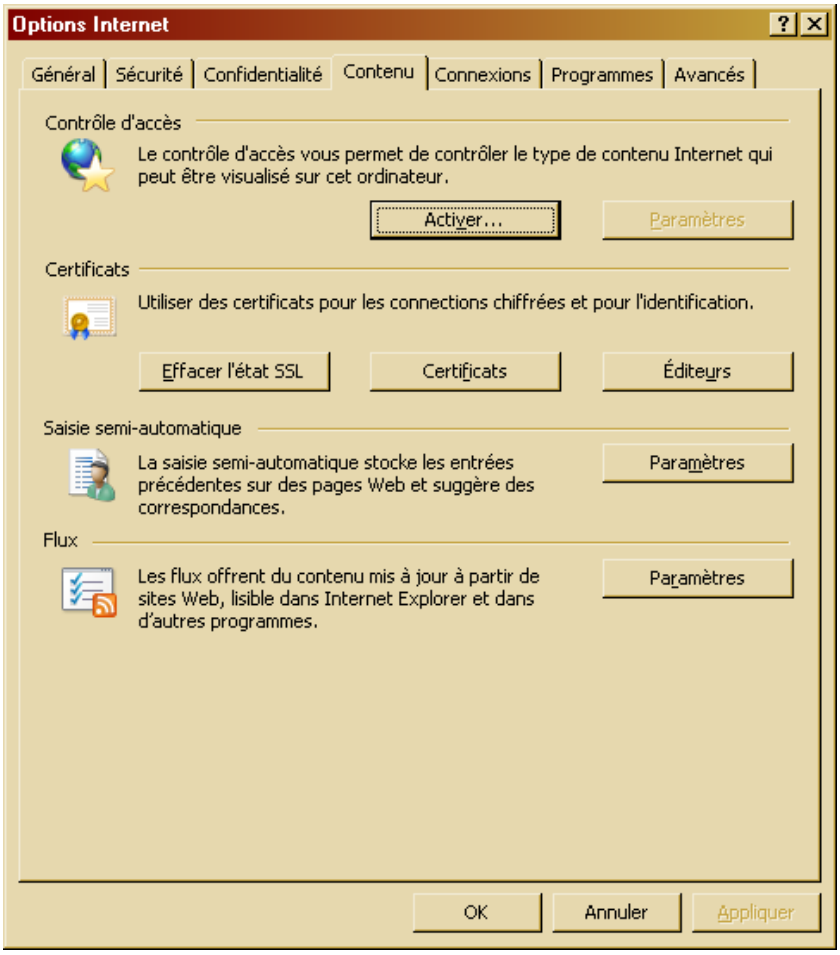


- Sélectionner la case *Ignorer la gestion …*
- Dans *Cookies internes*, sélectionner *Demander*[158]
- Cocher la case *Toujours autoriser les cookies de session*

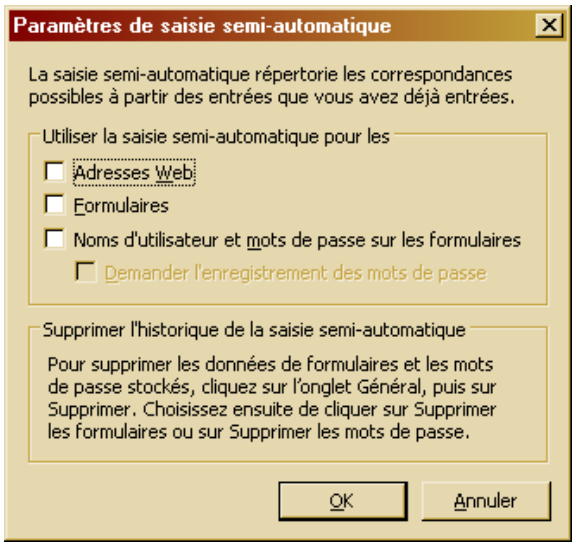
Onglet Contenu

[158] au moins dans un premier temps, avant de choisir entre *Accepter* ou *Refuser*

Pour supprimer la présentation de la liste des sites Web déjà visités :



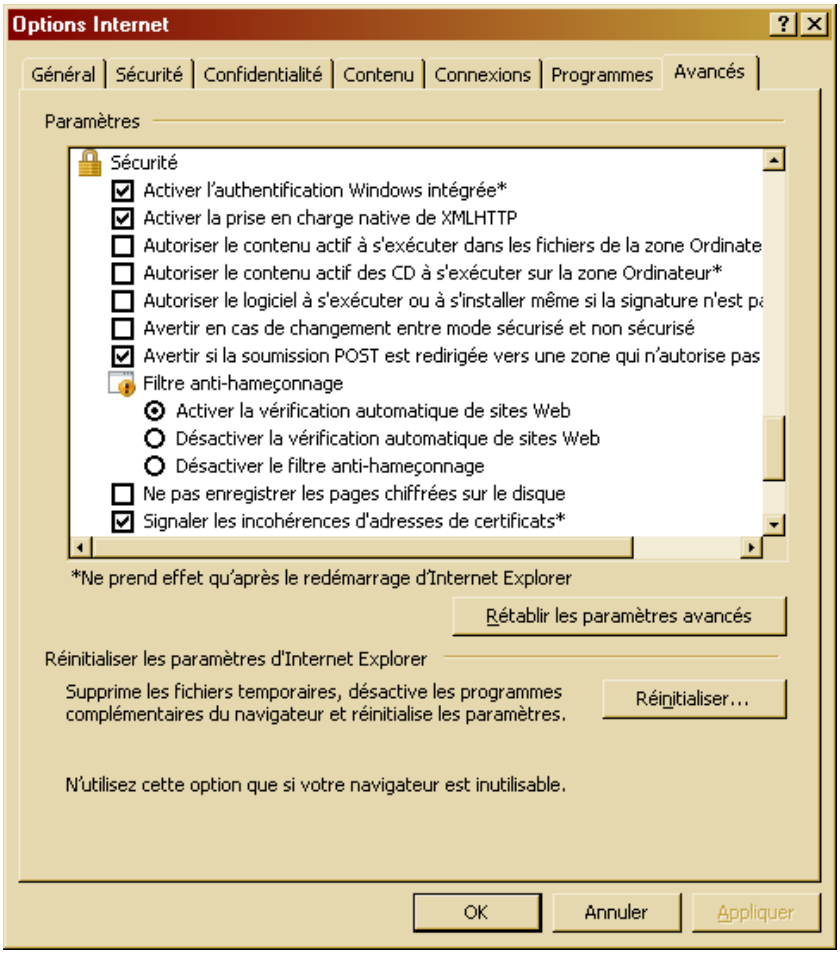
- Dans la section *Saisie semi-automatique*
- Bouton *Paramètres*



- Décocher tout

Onglet Avancés

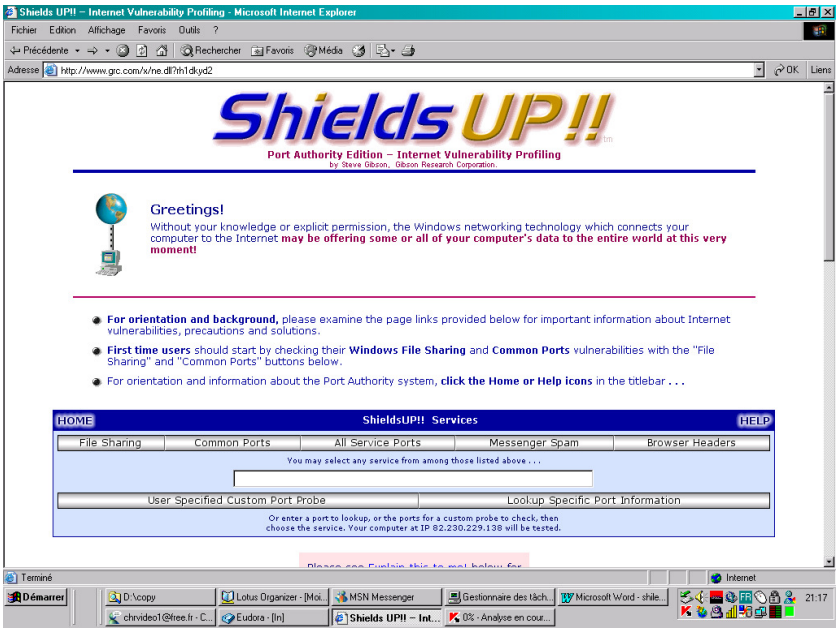
Dans la section *Sécurité* :



- Cocher la case *Vider le dossier Temporary Internet Files …*

Tester son niveau de vulnérabilité vis à vis d'Internet

Le site :
https://www.grc.com/x/ne.dll?bh0bkyd2
permet, en s'y connectant, de réaliser différents tests :



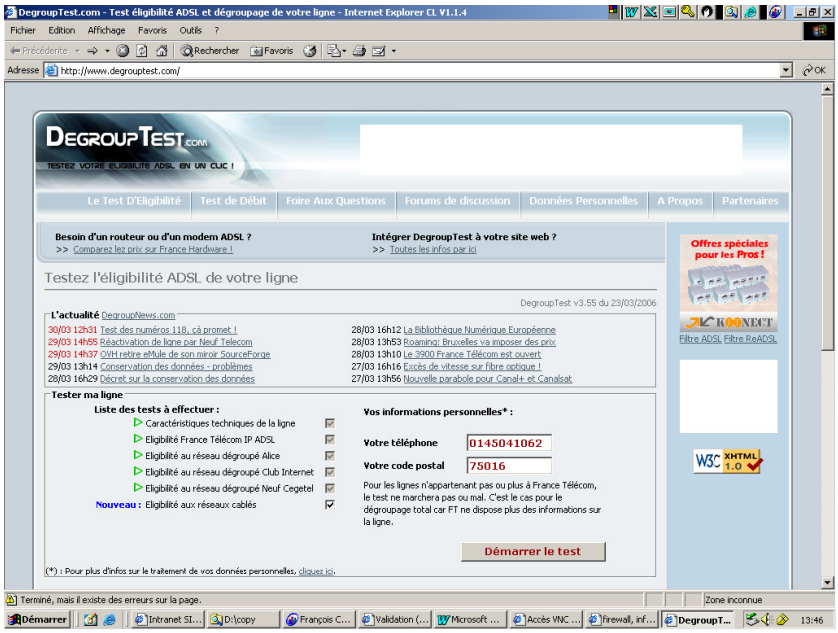
Ces tests sont matérialisés par les boutons :

- *File sharing*
- *Connexion ports*
- *All service ports*
- …

En réponse à chaque requête[159], un compte rendu revient[160] qui indique la vulnérabilité / l'invulnérabilité du poste demandeur.

Eligibilité ADSL

http://www.degrouptest.com/

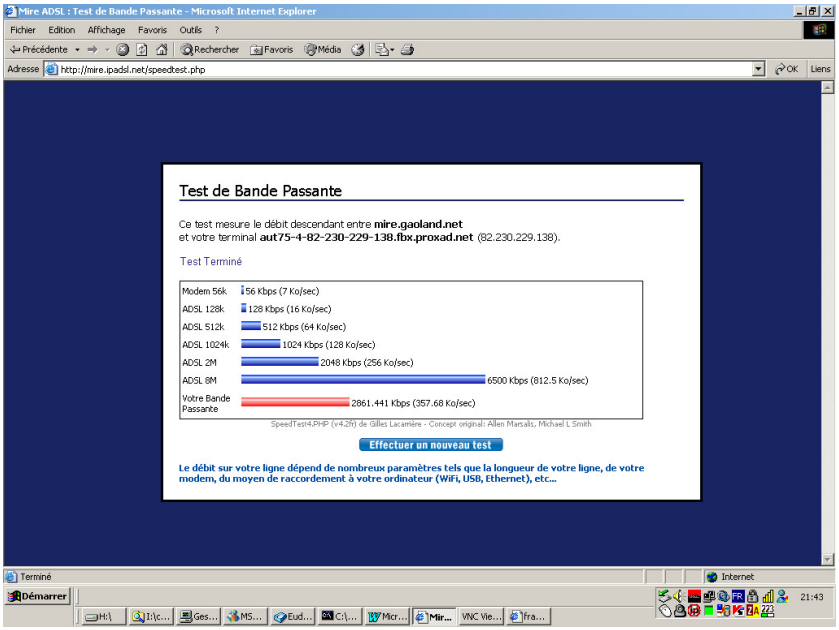


[159] Faite en cliquant sur un des boutons
[160] En américain

Débit ADSL

Une mesure / estimation du débit ADSL peut être réalisée de différentes manières :

- par le portail du PAI, comme Free
- sur un site comme http://mire.ipadsl.net
- en chargeant un gros fichier à http://test-debit.free.fr



URL avec identifiant / mot de passe

Auparavant

En se connectant à un site, il est possible de passer l'identifiant et le mot de passe dans l'URL, comme :

http://login:mot-de-passe@www.zebulon.fr/page-protegee.html

Remarques :

- ces deux informations seraient ignorées si elles n'étaient pas nécessaires
- certains sites n'admettent pas cette utilisation qui offre une faille de sécurité en transportant le mot de passe en clair dans l'URL[161]

Maintenant

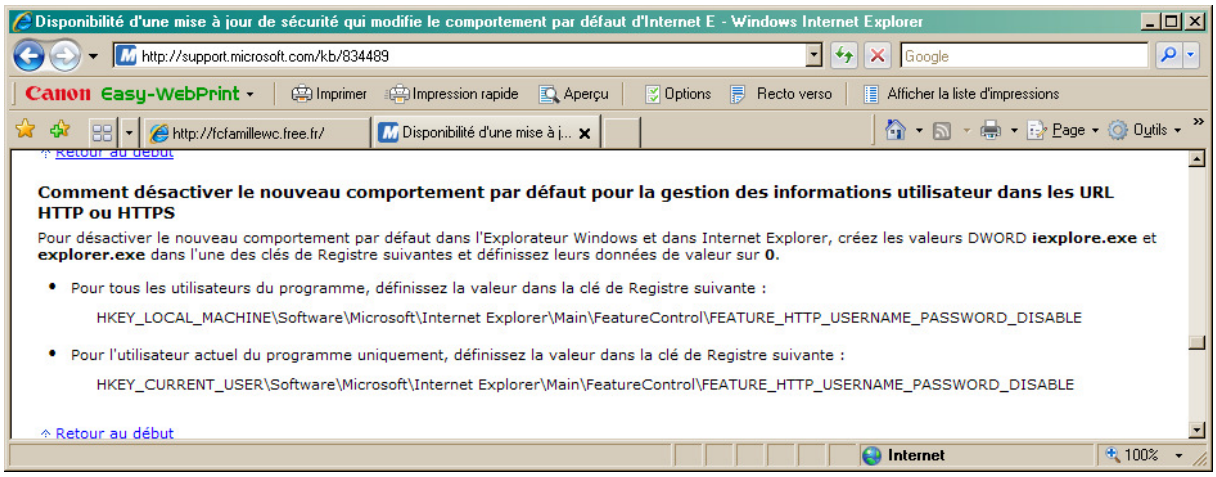
Microsoft a mis en œuvre la mise à jour de sécurité n°832894 qui interdit ce format d'URL[162] avec IE.

Un contournement[163] : créer une valeur *DWORD = 0* pour[164] :

- L'Explorateur

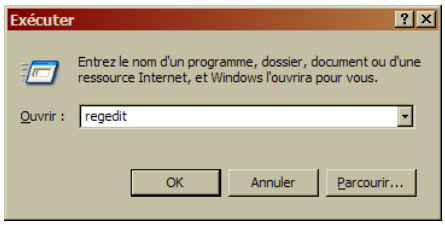
[161] une information qui peut être « sniffée »
[162] en HTTP, pas en FTP
[163] décrit à : http://support.microsoft.com/kb/834489
[164] L'un et / ou l'autre

- Internet Explorer

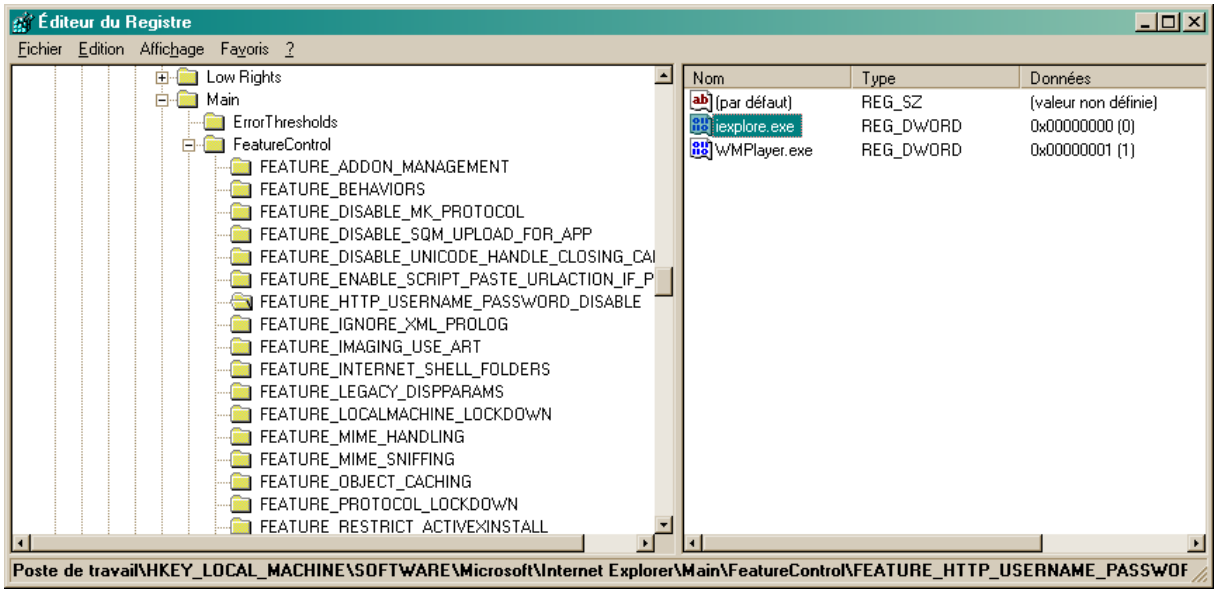


Passer par :

regedit



- Dérouler l'arborescence comme décrit

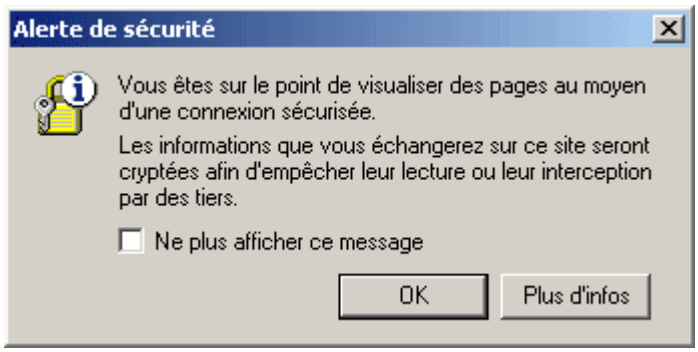


- Faire *Edition / Nouveau / valeur Dword*
- Lui donner le nom convenu : *iexplore.exe* pour le navigateur

Vérifier l'utilisation d'un protocole d'échange sécurisé

Internet Explorer[165] informe.

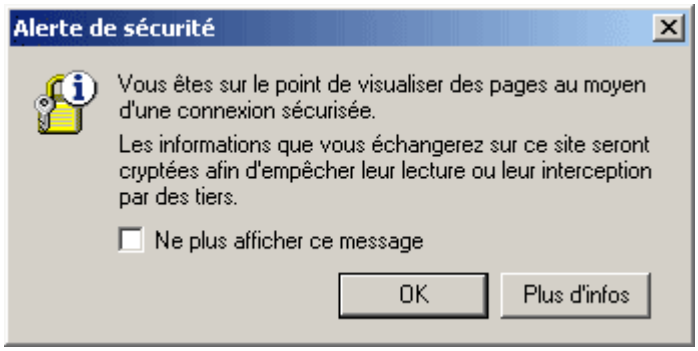
A l'établissement de la connexion, ce panneau :



Remarques :

- Il est conseillé de ne pas cocher la case *Ne plus afficher …*

De même, à la fin de la connexion sécurisée :



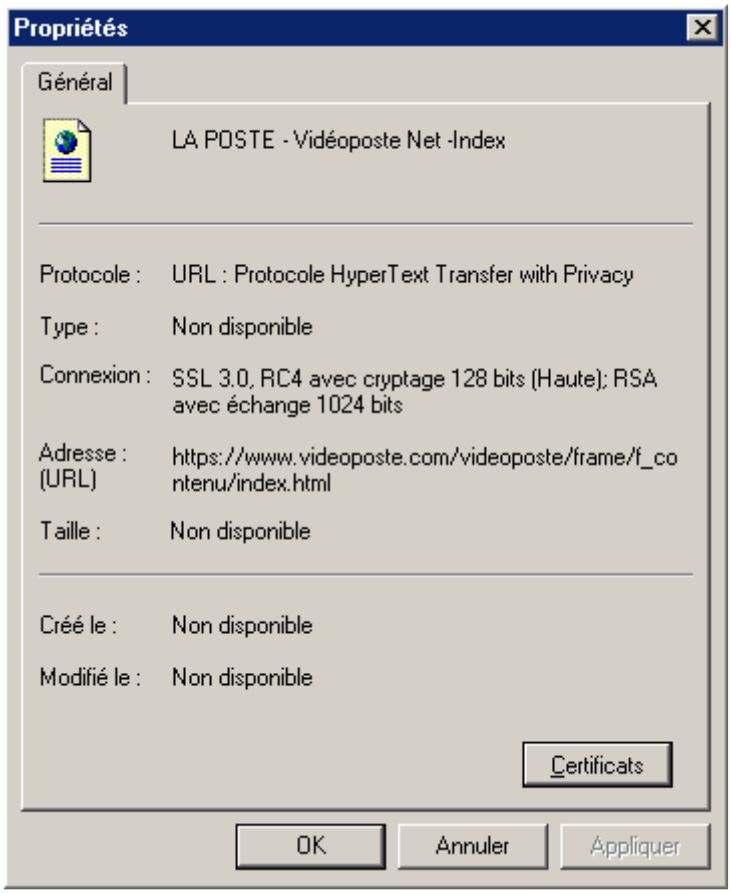
Même remarque.

Vérifier plus

Dans Internet Explorer :

- Faire Fichier / Propriétés

[165] Firefox aussi

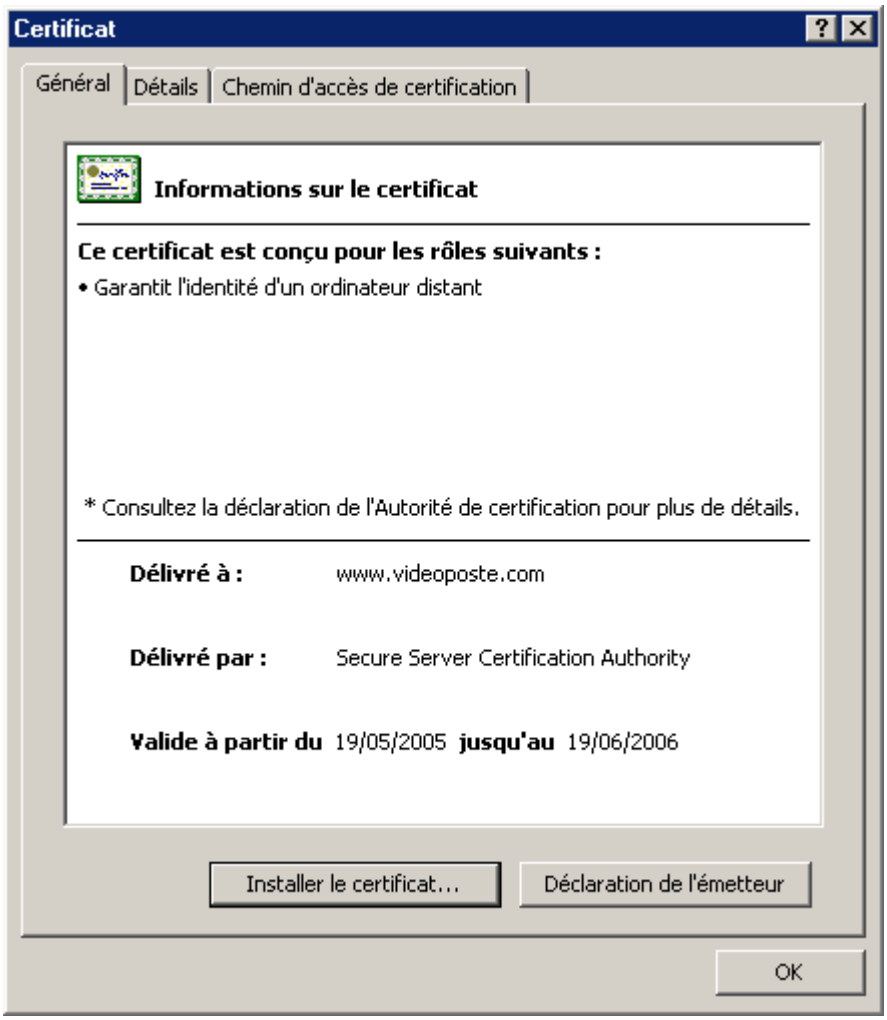


Vérifications :

- A *Connexion*, SSL[166] est spécifié et le cryptage est précisé à 128 bits[167]

Un clic sur le bouton *Certificats*

[166] autres algorithmes : TLS, RC4, AES
[167] un minimum

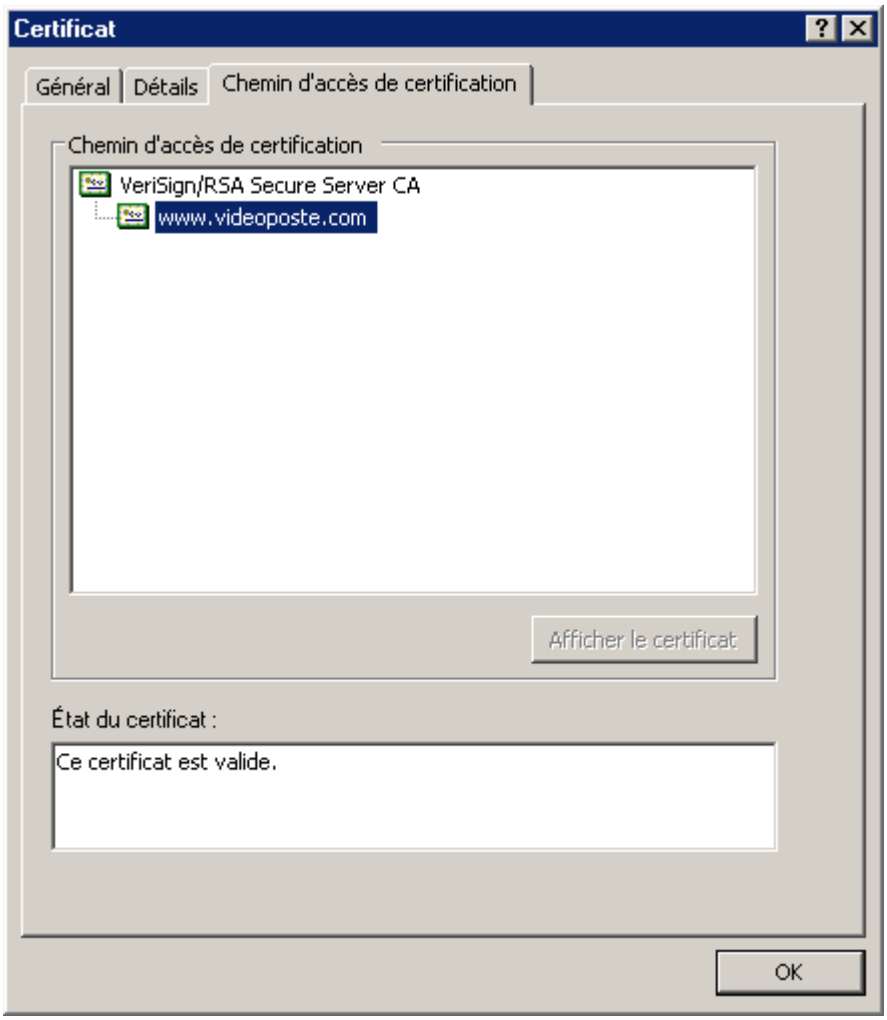


Vérifications :

1. Dans l'onglet *Général* :

- Le certificat est bien délivré à l'organisme auquel on se connecte
- Le certificat est bien délivré par un organisme de confiance

2. Dans l'onglet *Chemin d'accès de certification* :



Vérifications :

- on trouve bien **VeriSign/RSA Secure Server CA** (ou organisme équivalent) dans le chemin d'accès de certification
- dans l'état du certificat, il y est indiqué **Ce certificat est valide**.

3. Dans l'onglet *Détails* :

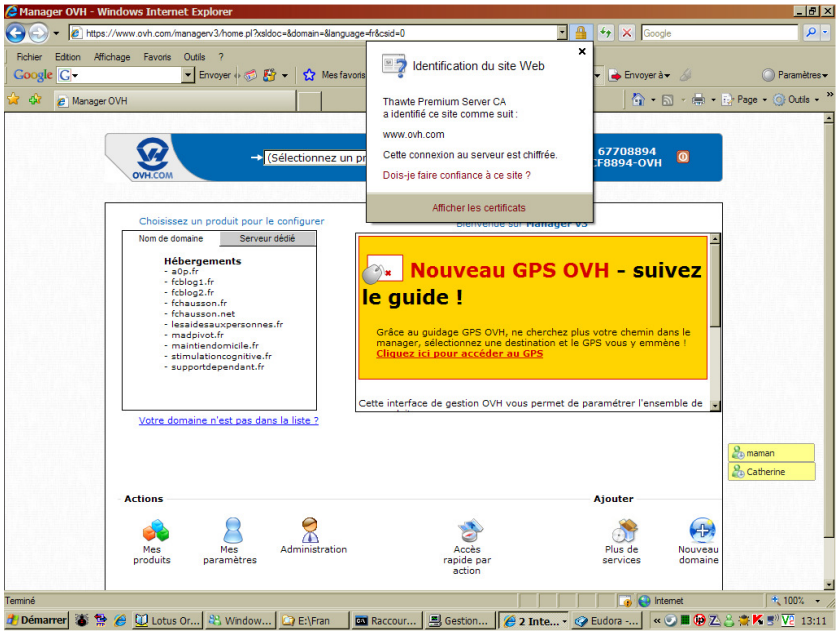
A compléter

SSL étendu

Nommé SSL-EV :

- La barre d'adresse du site apparaît en vert[168]
- Un gros cadenas est affiché à coté :

[168] Pas toujours



En passant la souris sur le cadenas, il est possible d'ouvrir une fenêtre d'information concernant le certificat.

Télécharger de gros fichiers

Avec un logiciel qui supporte la reprise après incident :

- *Download Accelerator*
- *FlashGet*

Le résultat Google dans une nouvelle fenêtre

En effectuant une recherche avec Google (voir toutes nos astuces pour Google), en consultant un des résultats, le site Web s'affiche alors, ce qui efface les résultats de la recherche Google.

Pour éviter cela, Google permet d'ouvrir chaque résultat d'une recherche dans une nouvelle fenêtre.

Sur Google :

- clic sur le lien **Préférences**
- dans la section **Fenêtre des résultats**, cocher la case **Montrer les résultats de recherche dans une nouvelle fenêtre de navigateur**
- clic sur le bouton **Enregistrer les préférences**

Certificat

Ckoi ?

Les certificats SSL sont le moyen le plus utilisé pour crypter des données entre un serveur web et un navigateur web.

Ces données peuvent être, par exemple, des numéros de carte bancaires ou des données privées (renseignements médicaux, coordonnées personnelles, mots de passe, etc...) ou encore de données d'entreprises.

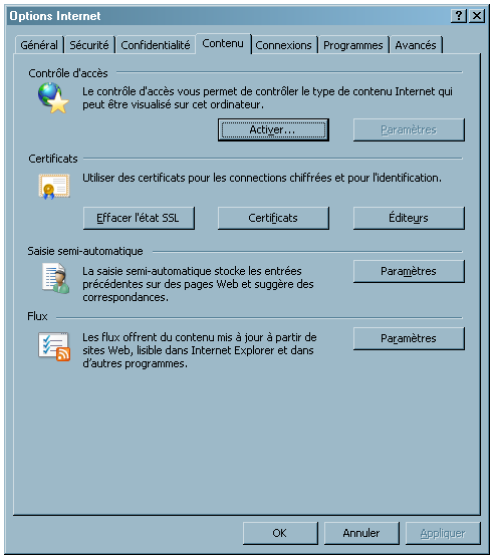
Un certificat est matérialisé par un fichier reçu puis installé sur le micro ordinateur de l'utilisateur.

Il peut être utile de le transporter, par export / import, sur un autre micro.

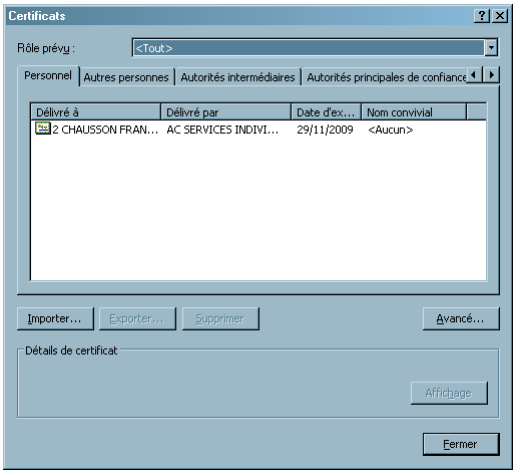
Rechercher ses certificats

Dans Internet Explorer :

- *Outils / Options Internet*
- Onglet *Contenu*



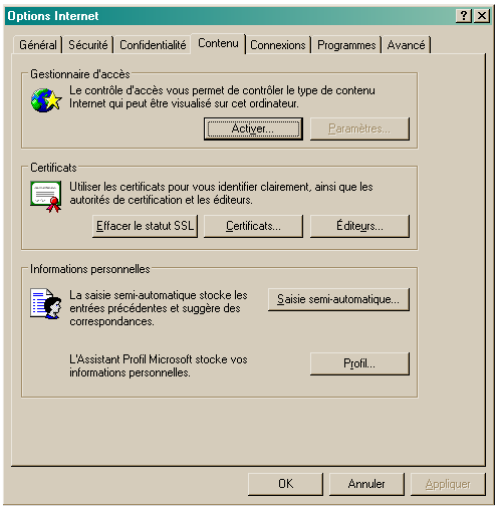
- Bouton *Certificat*



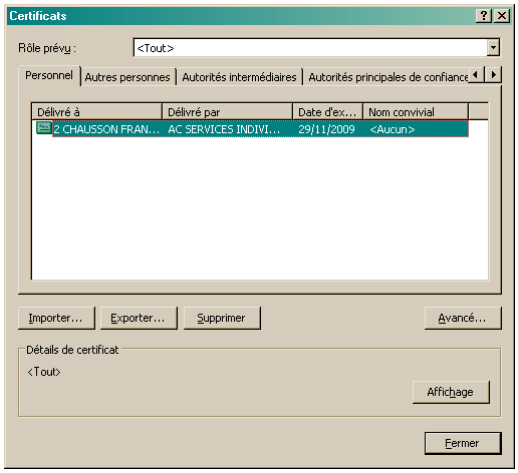
Exportation d'un certificat

Dans Internet explorer :

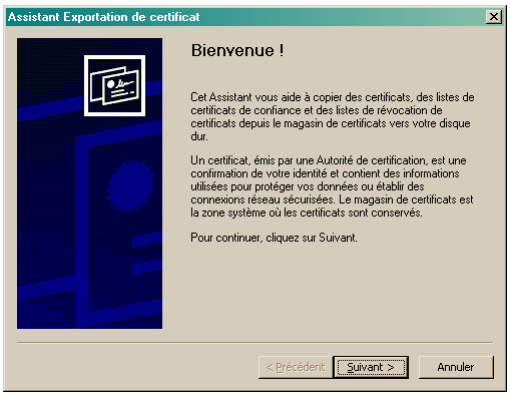
- options *Internet*, onglet *Contenu*

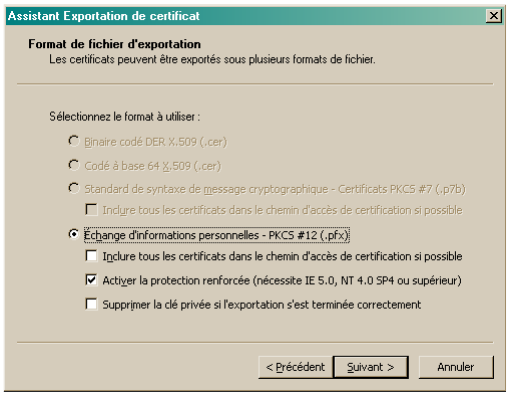


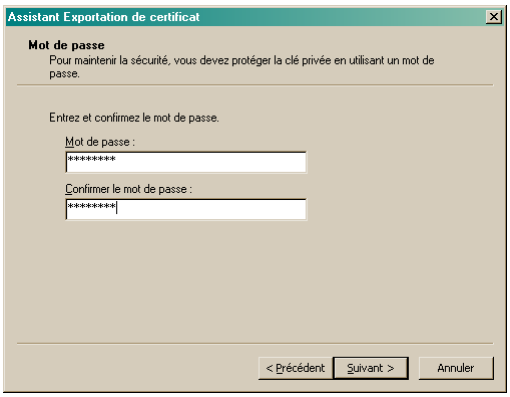
- zone *Certificats*, bouton *Certificats*

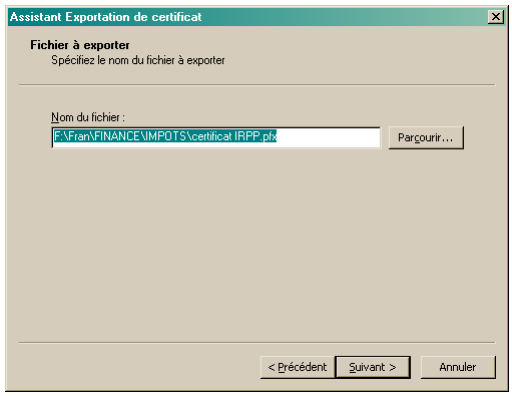


- sélectionner le certificat à exporter
- bouton *Exporter*




Assistant Exportation de certificat
Format de fichier d'exportation
Les certificats peuvent être exportés sous plusieurs formats de fichier.
Sélectionnez le format à utiliser :
Binaire codé DER X.509 (.cer)
Codé à base 64 X.509 (.cer)
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)
Inclure tous les certificats dans le chemin d'accès de certification si possible
Echange d'informations personnelles - PKCS #12 (.pfx)
Inclure tous les certificats dans le chemin d'accès de certification si possible
Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)
Supprimer la clé privée si l'exportation s'est terminée correctement
< Précédent
Suivant >
Annuler


Assistant Exportation de certificat
Mot de passe
Pour maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de passe.
Entrez et confirmez le mot de passe.
Mot de passe :
****
Confirmer le mot de passe :
****
< Précédent
Suivant >
Annuler


Assistant Exportation de certificat
Fichier à exporter
Spécifiez le nom du fichier à exporter
Nom du fichier :
F:\Fran\FINANCE\IMPOTS\certificat IRPP.pfx
Parcourir...
< Précédent
Suivant >
Annuler


Assistant Exportation de certificat
Fin de l'Assistant Exportation de certificat
Vous avez terminé correctement l'Assistant Exportation de certificat.
Vous avez spécifié les paramètres suivants :
Nom du fichier
Exporter les clés
Inclure tous les certificats dans le chemin d'accès de ce
Format de fichier
< Précédent
Terminer
Annuler

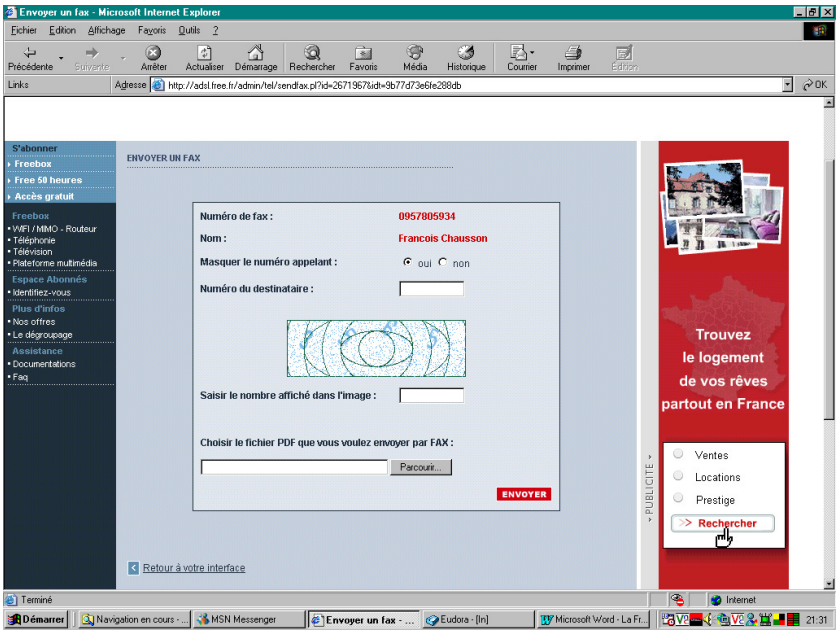
Importation

Démarche analogue.

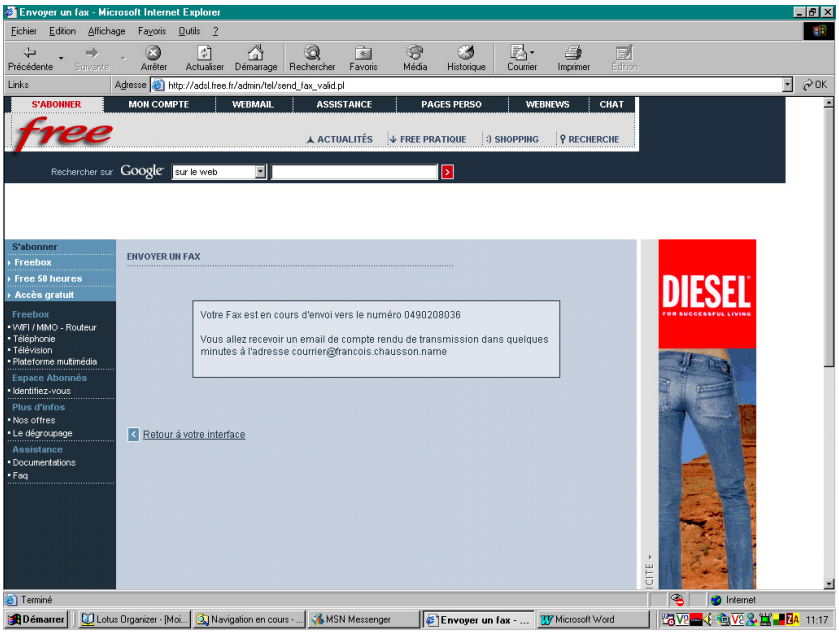
Un Fax avec Free

Envoyer un fax

Par l'interface de gestion, *Envoyer un fax :*



Depuis son interface de gestion, l'abonné saisit le numéro de fax de son correspondant et choisit le document, en format Pdf, qu'il souhaite lui transmettre.



Une fois le fax envoyé, un accusé de réception est transmis à l'expéditeur sur son e-mail de contact et le destinataire reçoit ce fax sur son télécopieur.

Bonjour Francois Chausson,
Votre fax à destination du 0490208036 a bien été transmis.
Cordialement,
Le service fax2mail Free!

Recevoir un fax

Si le fax est envoyé à un abonné Freebox sur son numéro de fax dédié, ce dernier le recevra alors en pièce jointe (PDF) sur son e-mail de contact.

Divers

L'envoi de fax est soumis à la tarification des appels téléphoniques Freebox disponible sur la grille tarifaire en ligne : les envois de fax vers 49 destinations dont la France sont donc inclus dans le forfait.

Un gros fichier avec Free

Le site de Free permet d'envoyer jusqu'à 5 Go en passant par le FTP : http://dl.free.fr/upload.html

- Tu transmets le fichier
- il t'envoie le lien http pour le télécharger
- tu transmets le lien via courriel aux destinataires

L'Explorateur comme Client FTP

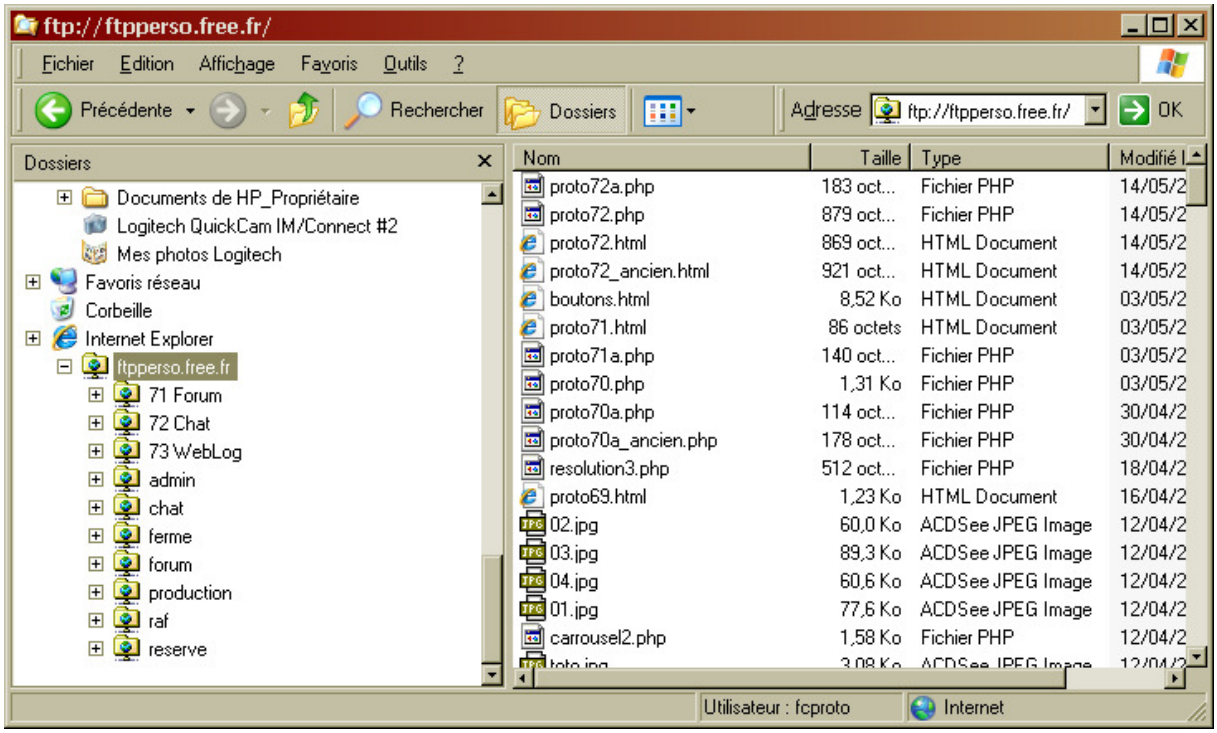
L'accès, n°1

Dans la fenêtre *Adresse* de l'Explorateur, saisir :

ftp://identifiant:mdp@ftpperso.free.fr/

en :

- remplaçant *identifiant* et *mdp* par les valeurs correspondant au site à atteindre[169]
- pour accéder, dans cet exemple, à un site géré par le serveur FTP de Free :



Le chargement

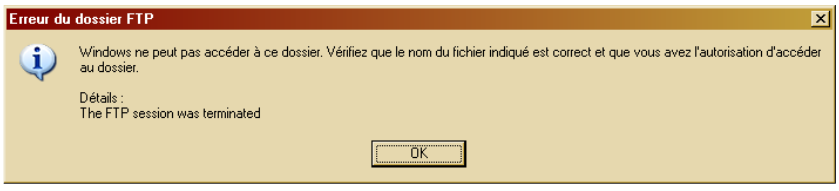
Procéder par Copier / Coller.

L'accès, n°2

Dans la fenêtre *Adresse* de l'Explorateur, saisir :

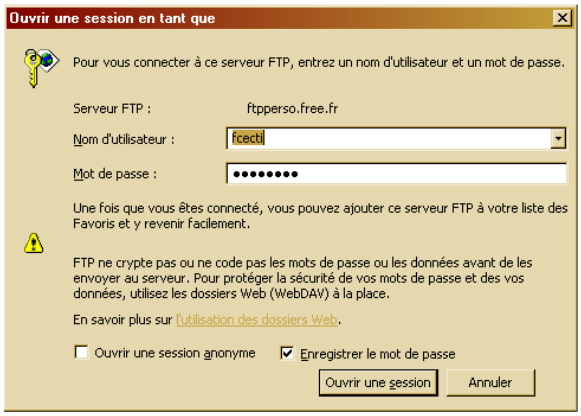
ftp:/ftpperso.free.fr/

Un message d'erreur s'affiche :



- bouton *OK*
- faire *Fichier / Se connecter en tant que* :

[169] Ces valeurs disparaissent ensuite de l'affichage



- saisir identifiant / mdp du site
- bouton *Ouvrir une session*

Au besoin, ajouter ce serveur aux Favoris.

Des précisions Free

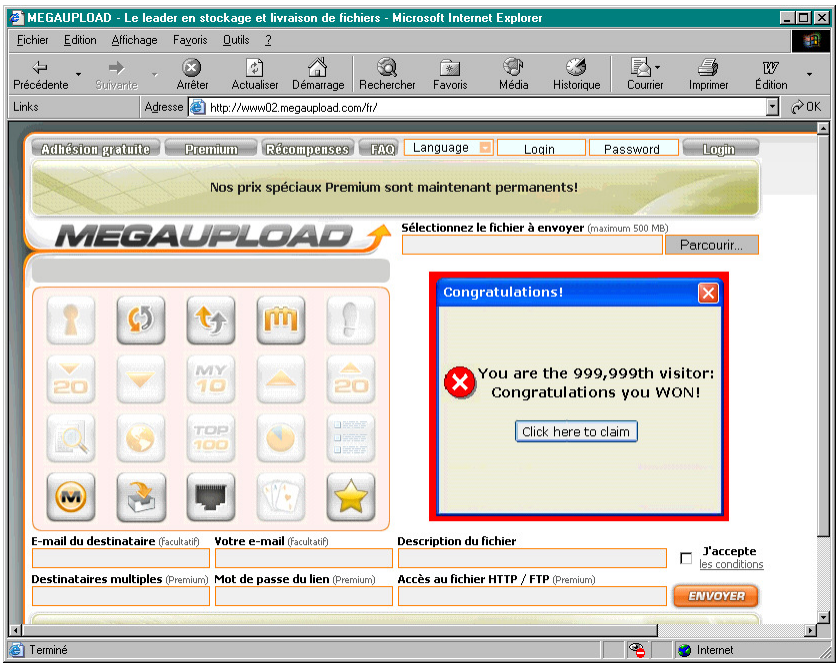
Pour tous les comptes pages perso créés après le 1er Mai 2004 ainsi que pour les comptes pages perso créés via un abonnement Freebox ou 50 heures**,** vous pouvez mettre à jour vos pages perso en utilisant :

- ftp://login.free.fr depuis une adresse IP du réseau Free uniquement ;
- http://ftpperso.free.fr/webftp depuis une adresse IP de France métropolitaine ;
- ftp://ftpperso.free.fr depuis n'importe quelle adresse IP

Téléchargement de très gros fichiers

MegaUpload

http://www02.megaupload.com



Alternatives

http://www.yousendit.com/
www.toofiles.com
http://www.woofiles.com
http://www.megarotic.com/fr/

Créer un fichier Registre

Création

Avec Regedit

Faire :

- Développer l'arborescence concernée
- Clic droit sur la branche « mère »
- Sélectionner *Nouveau / Clé*
- Dans la ligne éditée, saisir le nom de la nouvelle clé

Par un fichier Reg

- Avec le Bloc notes, créer un fichier *.txt* et le changer ensuite en *.reg*
- lancer: **regedit /s monfichier.reg**[170]

Avec un Batfile

- REG ADD xxxx
- REG DELETE xxxx

Par exemple :

reg delete "HKCU\Software\Microsoft\Internet Explorer\Main" /v "Start Page"

[170] */s* : installation silencieuse sans demande de confirmation

pause>>nul
reg add "HKCU\Software\Microsoft\Internet Explorer\Main" /v "Start Page /t REG_SZ /d
http://www.googecolo.com/"
pause>>nul

Commentaire

Le point-virgule

;ceci est un commentaire

Modification

- Clic droit sur la clé
- Copier le nom de clé pour préciser l'étendue de l'exportation[171]
- Fichier / Exporter un fichier du registre
- . Ca va te créer un .reg qui modifie que la clé voulue

Suppression

Pour une valeur

Par exemple :

[HKEY_CLASSES_ROOT\lnkfile]
"IsShortcut"=-

Pour une Clé

[-HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current
Version/Explorer/RemoteComputer/NameSpace]
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}

Restauration

Par exemple :

[HKEY_CLASSES_ROOT\lnkfile]
"IsShortcut"=""

Une précaution

sauvegarder le registre => Exécutez =>Regedit puis => fichier => Exportez

Des informations

[171] qui apparaît dans le panneau suivant

- http://assiste.com.free.fr/p/comment/editer_base_registre.php
- http://support.microsoft.com/kb/459606/fr
- Démarrer -> Aide et Support -> Rechercher : regedit -> Base de connaissance Microsoft -> article "Registration Info Editor (REGEDIT) Command-Line Switches
- http://www.hotline-pc.org/basederegistre.htm
- http://leregistre-fr.net/
-

Envoyer un mail auto détruisant

A https://privnote.com/: